

国際調査報告

(法 8 条、法施行規則第40、41条)
〔PCT 18 条、PCT 規則43、44〕

出願人又は代理人 の書類記号 5 2 2 1 9 6 W O 0 1	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220)及び下記5を参照すること。		
国際出願番号 PCT/JP00/09129	国際出願日 (日.月.年) 2 2 . 1 2 . 0 0	優先日 (日.月.年) 1 4 . 0 1 . 0 0	
出願人 (氏名又は名称) 三菱電機株式会社			

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT 18 条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 3 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない(第 I 欄参照)。

3. ☐ 発明の単一性が欠如している(第 II 欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。

☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。

☐ 第 III 欄に示されているように、法施行規則第47条(PCT 規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から 1 カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、
第 1 図とする。 ☒ 出願人が示したとおりである。

☐ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

This Page Blank (uspto)

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/10

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年
日本国公開実用新案公報 1971-2001年
日本国登録実用新案公報 1994-2001年
日本国実用新案登録公報 1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP, 9-298736 (松下電器産業株式会社) 18. 11月. 1997 (18. 11. 97) 第10頁右欄第28行目~第12頁左欄第31行目, 全図 (ファミリーなし)	1-7, 11-17, 21-23, 27-29, 33, 35, 37, 39, 41-44

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

30. 03. 01

国際調査報告の発送日

10.04.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5W

2956

電話番号 03-3581-1101 内線 3535

This Page Blank (uspto)

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	J P, 10-123950, A (富士ゼロックス株式会社) 15. 5月. 1998 (15. 05. 98) 第4頁右欄第38行目~第5頁左欄第27行目, 第21図	8, 10, 18, 20, 24, 26, 30, 32, 34, 36, 38, 40, 45-50
A	全文, 全図 & EP, 837383, A2 & US, 6161183, A	9, 19, 25, 31
X	J P, 8-248879, A (インターナショナル・ビジネス・マ シーンズ・コーポレーション) 27. 9月. 1996 (27. 09. 96) 第4頁右欄第33行目~第43行目, 全図 & EP, 725511, A2 & US, 5673319, A1	8-10, 18-20, 24-26, 30-32, 34, 36, 38, 40, 45-50
A	J P, 4-48336, A (富士通株式会社) 18. 2月. 1992 (18. 02. 92) 全文, 全図 (ファミリーなし)	1-50
A	J P, 2-73747, A (日本電気株式会社) 13. 3月. 1990 (13. 03. 90) 全文, 第1図 (ファミリーなし)	1-50
A	J P, 57-69344, A (日本電信電話公社) 28. 4月. 1982 (28. 04. 82) 全文, 全図 (ファミリーなし)	1-50
A	J P, 4-191935, A (株式会社東芝) 10. 7月. 1992 (10. 07. 92) 全文, 全図 (ファミリーなし)	1-50

This Page Blank (uspto)

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2001 年 7 月 19 日 (19.07.2001)

PCT

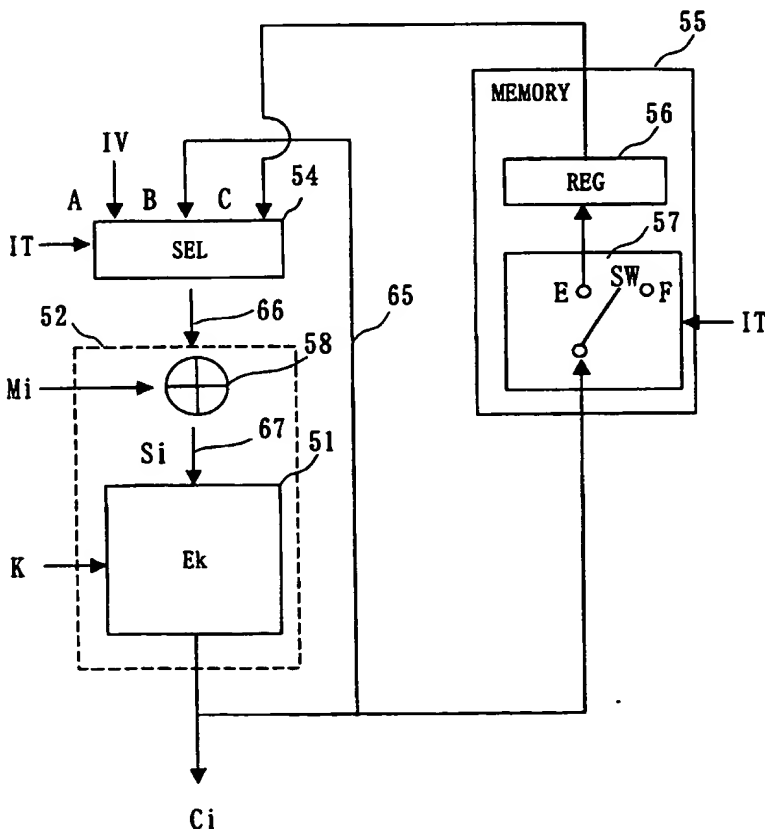
(10) 国際公開番号
WO 01/52472 A1

- (51) 国際特許分類: H04L 9/10 KAISHA) [JP/JP]; 〒100-8310 東京都千代田区丸の内二丁目2番3号 Tokyo (JP).
- (21) 国際出願番号: PCT/JP00/09129
- (22) 国際出願日: 2000 年 12 月 22 日 (22.12.2000) (72) 発明者; および (75) 発明者/出願人 (米国についてのみ): 反町 亨 (SORI-MACHI, Toru) [JP/JP]. 時田俊雄 (TOKITA, Toshio) [JP/JP]; 〒100-8310 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内 Tokyo (JP).
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ: 特願2000-5161 2000 年 1 月 14 日 (14.01.2000) JP (74) 代理人: 溝井章司, 外(MIZOI, Shoji et al.); 〒247-0056 神奈川県鎌倉市大船二丁目17番10号 NTA大船ビル 3F Kanagawa (JP).
- (71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI (81) 指定国 (国内): AU, CA, CN, JP, KR, MX, NO, SG, US.

[続葉有]

(54) Title: METHOD AND APPARATUS FOR ENCRYPTION, METHOD AND APPARATUS FOR DECRYPTION, AND COMPUTER-READABLE MEDIUM STORING PROGRAM

(54) 発明の名称: 暗号化装置及び暗号化方法及び復号装置及び復号方法及びプログラムを記録したコンピュータ読み取り可能な記録媒体



(57) Abstract: In order to encipher data while enciphering other data, a memory (55) is arranged in parallel to a feedback line (65) for feedback to a selector (54) from an enciphering module (51) using an encryption key (K). If an interrupt (IT) for processing plaintext block data (N_i) occurs during the processing of plaintext block data (M_i), the cryptogram block data (C_i) being in process when the interrupt (IT) occurs is stored in a register (56). When the processing of the plaintext block data N_i is completed, a selector (54) selects the cryptogram block data (C_i) stored in the memory (55), and the processing of plaintext block data (M_{i+1}) is started.

[続葉有]



(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

(57) 要約:

暗号化の最中に他のデータの暗号化を行うために、暗号鍵Kを用いた暗号化モジュール51からセクタ54にフィードバックするフィードバックライン65に対して並列に設けられたメモリ55を配置する。平文ブロックデータ M_i を処理中に他のデータの平文ブロックデータ N_i を処理する割り込みITが発生した場合には、割り込みITが発生したときの暗号文ブロックデータ C_i をレジスタ56に記憶させ、平文ブロックデータ N_i の処理が終了した時点でメモリ55に記憶した暗号文ブロックデータ C_i をセクタ54に選択させることにより平文ブロックデータ M_{i+1} の処理を開始する。

明 細 書

暗号化装置及び暗号化方法及び復号装置及び復号方法及びプログラム
を記録したコンピュータ読み取り可能な記録媒体

5

技術分野

この発明は、暗号化復号装置及び暗号化復号方法に関するものである。
特に、データの暗号化復号の最中に他のデータの暗号化復号ができる
発明に関するものである。

10

背景技術

図43は、Cipher Block Chaining Mode
(以下、CBCモードという)による暗号化装置を示す図である。

図43に示すCBCモードでの暗号方法は、64ビットの平文ブロッ
クデータ M_i をブロック単位で入力して、暗号鍵 K を用いた暗号化モジ
15 ュール51により暗号化し、更に、この暗号化された暗号文ブロックデ
ータ C_i と次の平文ブロックデータ M_{i+1} との排他的論理和を演算し、
排他的論理和の演算結果を次の暗号化の入力として、暗号鍵 K を用いた
暗号化モジュール51に供給することにより暗号化する方法である。そ
20 して、この処理を繰り返して次々と連鎖させることにより、平文 M 全体
を暗号文 C に暗号化するものである。

図44は、CBCモードを用いた復号装置を示す図である。

図44に示す復号装置は、図43に示す暗号化装置により暗号化され
た暗号文を復号する装置である。暗号文ブロックデータ C_i が暗号鍵 K
25 を用いた復号モジュール71に入力され、イニシャルバリュー IV との
排他的論理和が計算され、平文ブロックデータ M_i が復号される。暗号

文ブロックデータ C_2 が入力された場合には、暗号鍵 K を用いた復号モジュール 71 で復号され、先に入力され、レジスタ 111 に保存された暗号文ブロックデータ C_1 との排他的論理和がとられ、平文ブロックデータ M_2 を復号する。

- 5 なお、レジスタ 111 は、セクタ 73 の内部に設けられていてもよい。

平文ブロックデータを M_i ($i = 1, 2, \dots, n$)、暗号文ブロックデータを C_i ($i = 1, 2, \dots, n$) とし、暗号鍵 K を用いた暗号化処理を E_K 、暗号鍵 K を用いた復号処理を D_K とすると、CBC モードは次式で表される。

$$C_1 = E_K (M_1 \oplus IV)$$

$$C_i = E_K (M_i \oplus C_{i-1}) \quad (i = 2, 3, \dots, n)$$

$$M_1 = D_K (C_1) \oplus IV$$

$$M_i = D_K (C_i) \oplus C_{i-1} \quad (i = 2, 3, \dots, n)$$

- 15 ここで、 \oplus は排他的論理和演算である。また、 IV (Initial Value) は初期値であり、最初の暗号化と復号の際に用いられる。イニシャルバリュー IV は、暗号化側と復号側で同一の値を用いる。

- 20 図 45 は、Output Feedback Mode (以下、OFB モードという) の暗号化装置を示す図である。

図 46 は、OFB モードの復号装置を示す図である。

図 47 は、Cipher Feedback Mode (以下、CFB モードという) の暗号化装置を示す図である。

図 48 は、CFB モードの復号装置を示す図である。

- 25 なお、レジスタ 111 は、セクタ 73 の内部に設けられていてもよい。

図49は、CBCモードの暗号化装置を用いて平文Mと平文Nを暗号化する手順を示す図である。

ここでは、平文Mが平文ブロックデータ M_1 、平文ブロックデータ M_2 、平文ブロックデータ M_3 から構成されており、平文Nが平文ブロックデータ N_1 のみで構成されている場合を説明する。

平文ブロックデータ M_1 の暗号化がスタートすると、暗号文ブロックデータ C_1 が出力されるとともに、暗号文ブロックデータ C_1 は、平文ブロックデータ M_2 の暗号化に用いられる。このように、暗号文ブロックデータ C_i は、平文ブロックデータ M_{i+1} の暗号化にフィードバックされて連鎖処理が行われる。従って、平文ブロックデータ M_1 から平文ブロックデータ M_3 までの暗号化が終わらなければ、平文ブロックデータ N_1 の暗号化を行うことができない。

図50は、図49と同様に、CBCモードで暗号化を行う場合を示している。

図50の場合は、平文ブロックデータ M_1 、平文ブロックデータ M_2 、平文ブロックデータ M_3 の各データが準備されるのに時間がかかってしまう場合を示している。一方、暗号化処理は、次の平文ブロックデータ M_{i+1} が準備できる前に終了しており、アイドル時間（例えば、 $T_1 \sim T_2$ 、 $T_3 \sim T_4$ の時間）が発生してしまう場合を示している。このように、アイドル時間が発生する場合でも、暗号文ブロックデータ C_i が次の平文ブロックデータ M_{i+1} にフィードバックされる連鎖処理を行わなければならないため、平文ブロックデータ N_1 の処理は平文ブロックデータ M_3 の処理が終了してからでなければ行えない。

図51は、データの秘匿処理とデータの完全性を保証する処理を示す図である。平文Mは、例えば、OFBモードの暗号装置により暗号文Cに暗号化される。CBCモードの暗号装置により認証子Pが演算され、

暗号文Cの最後に認証子Pが付加される。暗号化され、かつ、認証子P
が付加されたデータを受信した場合には、暗号文Cから平文MをOFB
モードの復号装置により復号するとともに、暗号文CからCBCモード
の復号装置により認証子Pを演算し、伝送されてきた認証子Pと同一か
5 否かを比較することにより、伝送されてきたCが改竄されていないこと
を確認することができる。

図52は、図51に示した秘匿処理と認証子演算処理の手順を示す図
である。

平文ブロックデータ M_1 ～平文ブロックデータ M_3 は、順に暗号文ブ
10 ロックデータ C_1 ～暗号文ブロックデータ C_3 に暗号化される。その後
、暗号文ブロックデータ C_1 ～暗号文ブロックデータ C_3 を順に入力し
て認証子Pが演算される。

図42～図48に示した各モードの暗号化装置及び復号装置は、前の
ブロックデータの暗号化復号されたデータをフィードバックさせて次の
15 ブロックデータの暗号化復号処理に利用しなければならないため、一旦
暗号化処理又は復号処理がスタートしてしまうと、その全体の処理が終
了しない限り、他の暗号化処理又は復号処理をスタートさせることがで
きないという課題があった。従って、先にスタートした暗号化復号処
理が長時間要するものである場合には、後からスタートする暗号化復号処
20 理が長時間待たされてしまうという課題があった。

また、暗号化復号されるデータが準備される時間に比べて、暗号化復
号処理に要する時間が短い場合には、暗号化復号化装置にアイドル時間
が発生してしまうという課題があった。

また、秘匿処理と完全性保証処理を行う場合には、秘匿処理を行って
25 から完全性保証処理を行わなければならない、処理時間がかかってしまう
という課題があった。

この発明の好適な実施の形態においては、あるデータの暗号化復号処理の最中に他のデータの暗号化復号処理を行える暗号化装置、復号装置及び暗号化方法及び復号方法を得ることを目的とする。

また、この発明の好適な実施の形態においては、優先度の高いデータの暗号化復号を優先的に行えるようにすることを目的とする。

また、この発明の好適な実施の形態においては、秘匿処理と完全性保証処理を並列的に高速に行えるようにすることを目的とする。

発明の開示

10 この発明に係る暗号化装置は、第1の処理データと、第2の処理データとの暗号化処理をする暗号化装置において、

暗号化処理の状態を記憶するメモリを備え、

第1の処理データの暗号化処理が完了する前に第2の処理データの暗号化処理を開始するとともに、第2の処理データの暗号化処理を開始する場合に第1の処理データの暗号化処理の状態を上記メモリに記憶させ、第1の処理データの暗号化処理を再開する場合に、暗号化装置の暗号化処理の状態を、メモリに記憶した第1の処理データの暗号化処理の状態に復帰させてから第1の処理データの暗号化処理を再開することを特徴とする。

20

上記暗号化装置は、第2の処理データの暗号化処理の完了する前に第1の処理データの暗号化処理を再開するとともに、上記メモリは、第1の処理データの暗号化処理を再開する場合に第2の処理データの暗号化処理状態を記憶し、第2の処理データの暗号化処理を再開する場合は、暗号化装置の暗号化処理の状態を、メモリに記憶した第2の処理データの暗号化処理の状態に復帰させてから第2の処理データの暗号化処理を再

25

開することを特徴とする。

上記第 1 の処理データは、第 1 の平文であり、上記第 2 の処理データは、第 2 の平文であることを特徴とする。

5

上記暗号化装置は、割り込みにより第 2 の処理データの暗号化処理を開始することを特徴とする。

この発明に係る暗号化装置は、平文Mを構成する平文ブロックデータ
10 M_i ($i = 1, 2, 3, \dots$) と平文Nを構成する平文ブロックデータ N_j ($j = 1, 2, 3, \dots$) とを暗号化する暗号化装置において、

平文Mの暗号化処理中に平文Nの暗号化要求を平文Mの暗号化処理完了前に受け付けるメカニズムと、

15 平文ブロックデータ M_i の暗号化処理を行い暗号文ブロックデータ C_i を出力する暗号化ユニットと、

暗号化ユニットから出力された暗号文ブロックデータ C_i をフィードバックラインを介し暗号化ユニットにフィードバックするフィードバックループと、

20 フィードバックループのフィードバックラインと並列に設けられ、上記平文Nの暗号化要求を受け付け、平文Nのいずれかの平文ブロックデータの暗号化処理を開始することにより、上記平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化されない場合、フィードバックされる暗号文ブロックデータ C_i を記憶するメモリと、

25 平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化される場合は、上記フィードバックループのフィードバックライン

によりフィードバックされる暗号文ブロックデータ C_i を選択してフィードバックループに供給し、上記平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化されず、平文 N のいずれかの平文ブロックデータの次に暗号化される場合は、上記メモリに記憶された暗号文ブロックデータ C_i を選択してフィードバックループに供給するセレクトと

5 を備えたことを特徴とする。

上記メモリは、

10 複数の平文に対応した複数のレジスタと、

 暗号化処理をする平文に対応してレジスタを切り替えるスイッチと

 を備えたことを特徴とする。

この発明に係る暗号化方法は、暗号化モジュールから出力される暗号文ブロックデータ C_i ($i = 1, 2, 3, \dots$) を用いて第 1 の平文 M の平文ブロックデータ M_i ($i = 1, 2, 3, \dots$) を暗号化する工程と、

15 上記平文ブロックデータ M_i を暗号化している途中で又は平文ブロックデータ M_i を暗号化した後に、第 1 の平文 M の平文ブロックデータ M_{i+1} の暗号化に用いられる暗号文ブロックデータ C_i をメモリに記憶する工程と、

 上記平文ブロックデータ M_{i+1} の暗号化に用いられる暗号文ブロックデータ C_i をメモリに記憶した後に、第 2 の平文 N の少なくとも 1 つの平文ブロックデータを暗号化する工程と、

20 上記第 2 の平文 N の少なくとも 1 つの平文ブロックデータを暗号化した後に、メモリに記憶された、平文ブロックデータ M_{i+1} の暗号化に用

25 上記第 2 の平文 N の少なくとも 1 つの平文ブロックデータを暗号化した後に、メモリに記憶された、平文ブロックデータ M_{i+1} の暗号化に用

いられる暗号文ブロックデータ C_i を入力し、暗号化モジュールを用いて第1の平文Mの平文ブロックデータ M_{i+1} を暗号化する工程とを備えたことを特徴とする。

- 5 この発明に係る暗号化装置は、1つ以上の平文ブロックデータからなる平文を暗号化ユニット暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化装置において、

10 平文ブロックデータを暗号化ユニットにより暗号化したときに暗号化ユニットが出力した暗号文ブロックデータ C_i を暗号化ユニットへフィードバックする第1のフィードバックループを有し、平文ブロックデータを入力し、第1のフィードバックループにより暗号文ブロックデータ C_i をフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化部と、

15 認証子演算途中結果をフィードバックする第2のフィードバックループを有し、暗号化部から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第2のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成部とを備えたことを特徴とする。

20

上記暗号化部と認証子生成部とは、1つの暗号化モジュールと、1つのフィードバックループとを兼用して暗号化処理と認証子生成処理とを交互に行うとともに、

上記1つのフィードバックループは、

25 暗号化処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

暗号化処理と認証生成処理とを交互に実行するために、メモリから暗号化処理と認証子生成処理との結果を交互に選択して暗号化モジュールに出力するセレクタとを備えたことを特徴とする。

5

この発明に係る暗号化方法は、1つ以上の平文ブロックデータからなる平文を暗号化ユニットにより暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化方法において、

10 平文ブロックデータを暗号化ユニットにより暗号化したときに暗号化ユニットが出力した暗号文ブロックデータ C_i を暗号化ユニットへフィードバックする第1のフィードバック工程を有し、平文ブロックデータを入力し、第1のフィードバックループにより暗号文ブロックデータ C_i をフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化工程と、

15 認証子演算途中結果をフィードバックする第2のフィードバック工程を有し、暗号化工程から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第2のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成工程と
20 を備えたことを特徴とする。

この発明に係る復号装置は、第1の処理データと、第2の処理データとの復号処理をする復号装置において、

復号処理の状態を記憶するメモリを備え、

25 第1の処理データの復号処理が完了する前に第2の処理データの復号処理を開始するとともに、第2の処理データの復号処理を開始する場合

に第1の処理データの復号処理の状態を上記メモリに記憶させ、第1の処理データの復号処理を再開する場合に、復号装置の復号処理の状態を、メモリに記憶した第1の処理データの復号処理の状態に復帰させてから第1の処理データの復号処理を再開することを特徴とする。

5

上記復号装置は、第2の処理データの復号処理の完了する前に第1の処理データの復号処理を再開するとともに、上記メモリは、第1の処理データの復号処理を再開する場合に第2の処理データの復号処理状態を記憶し、第2の処理データの復号処理を再開する場合は、復号装置の復
10 号処理の状態を、メモリに記憶した第2の処理データの復号処理の状態に復帰させてから第2の処理データの復号処理を再開することを特徴とする。

上記第1の処理データは、第1の暗号文であり、上記第2の処理データは、第2の暗号文であることを特徴とする。
15

上記復号装置は、割り込みにより第2の処理データの最初のブロックデータの復号処理を開始することを特徴とする。

20 この発明に係る復号装置は、暗号文Cを構成する暗号文ブロックデータ C_i ($i = 1, 2, 3, \dots$)と暗号文Dを構成する暗号文ブロックデータ D_j ($j = 1, 2, 3, \dots$)とを復号する復号装置において、

暗号文Cの復号処理中に暗号文Dの復号要求を任意の時点で受け付けるメカニズムと、
25

暗号文ブロックデータ C_i の復号処理を行い平文ブロックデータ M_i

を出力する復号ユニットと、

暗号文ブロックデータ C_{i+1} を復号するための暗号文ブロックデータ C_i をフィードバックラインを介し復号ユニットにフィードバックするフィードバックループと、

- 5 フィードバックループのフィードバックラインと並列に設けられ、上記暗号文Dの復号要求を受け付け、暗号文Dのいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号されない場合、フィードバックされる暗号文ブロックデータ C_i を記憶するメモリと、
- 10 暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号される場合は、上記フィードバックループのフィードバックラインによりフィードバックされる暗号文ブロックデータ C_i を選択してフィードバックループに供給し、上記暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号されず、暗号文Dのいずれかの
- 15 暗号文ブロックデータの次に復号される場合は、上記メモリに記憶された暗号文ブロックデータ C_i を選択してフィードバックループに供給するセレクトと
- を備えたことを特徴とする。

- 20 上記メモリは、
- 複数の暗号文に対応した複数のレジスタと、
- 復号処理をする暗号文に対応してレジスタを切り替えるスイッチと
- を備えたことを特徴とする。

- 25 この発明に係る復号方法は、復号モジュールを用いて第1の暗号文Cの暗号文ブロックデータ C_i ($i = 1, 2, 3, \dots$) を復号する工

程と、

上記暗号文ブロックデータ C_i を復号している途中で又は暗号文ブロックデータ C_i を復号した後に、第1の暗号文Cの暗号文ブロックデータ C_{i+1} の復号に用いられる暗号文ブロックデータ C_i をメモリに記憶

5 する工程と、

上記暗号文ブロックデータ C_{i+1} の復号に用いられる暗号文ブロックデータ C_i をメモリに記憶した後に、第2の暗号文Dの少なくとも1つの暗号文ブロックデータを復号する工程と、

10 上記第2の暗号文Dの少なくとも1つの暗号文ブロックデータを復号した後に、メモリに記憶された、暗号文ブロックデータ C_{i+1} の復号に用いられる暗号文ブロックデータ C_i を入力し、復号モジュールを用いて第1の暗号文Cの暗号文ブロックデータ C_{i+1} を復号する工程とを備えたことを特徴とする。

15 この発明に係る復号装置は、1つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号装置において、

20 復号モジュールによりデータを復号したときに生成したモジュール出力ブロックデータ T_i を復号モジュールへフィードバックする第1のフィードバックループを有し、暗号文ブロックデータを入力し、第1のフィードバックループによりモジュール出力ブロックデータ T_i をフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号部と、

25 認証子演算途中結果をフィードバックする第2のフィードバックループを有し、復号部に入力される暗号文ブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し

、第2のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成部と
を備えたことを特徴とする。

5

上記復号部と認証子生成部とは、1つの復号モジュールと、1つのフィードバックループとを兼用して復号処理と認証子生成処理とを交互に行うとともに、

上記1つのフィードバックループは、

10 復号処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

復号処理と認証生成処理とを交互に実行するために、メモリから復号処理と認証子生成処理との結果を交互に選択して復号モジュールに出力するセレクトと

15 を備えたことを特徴とする。

この発明に係る復号方法は、1つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号方法において、

20 復号モジュールによりデータを復号したときに生成したモジュール出力ブロックデータ T_i を復号モジュールへフィードバックする第1のフィードバック工程を有し、暗号文ブロックデータを入力し、第1のフィードバックループによりモジュール出力ブロックデータ T_i をフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号工程と

25

認証子演算途中結果をフィードバックする第2のフィードバック工程

を有し、復号工程に入力される暗号文ブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第2のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成工程と

5 を備えたことを特徴とする。

この発明に係る暗号化装置は、平文Mを構成する平文ブロックデータ M_i ($i = 1, 2, 3, \dots$) と平文Nを構成する平文ブロックデータ N_j ($j = 1, 2, 3, \dots$) とを暗号化する暗号化装置において、

10 、

平文Mの暗号化処理中に平文Nの暗号化要求を平文Mの暗号化処理完了前に受け付けるメカニズムと、

暗号化処理を行ったデータをモジュール出力ブロックデータ T_i として出力する暗号化モジュールと、

15 、

暗号化モジュールから出力されたモジュール出力ブロックデータ T_i をフィードバックラインを介し暗号化モジュールにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記平文Nの暗号化要求を受け付け、平文Nのいずれかの平文ブロックデータの暗号化処理を開始することにより、上記平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化されない場合、フィードバックされるモジュール出力ブロックデータ T_i を記憶するメモリと、

20 、

平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化される場合は、上記フィードバックループのフィードバックライン

25

によりフィードバックされるモジュール出力ブロックデータ T_i を選択してフィードバックループに供給し、上記平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化されず、平文 N のいずれかの平文ブロックデータの次に暗号化される場合は、上記メモリに記憶されたモジュール出力ブロックデータ T_i を選択してフィードバックループに供給するセクタと

5 を備えたことを特徴とする。

上記メモリは、

10 複数の平文に対応した複数のレジスタと、

 暗号化処理をする平文に対応してレジスタを切り替えるスイッチと

 を備えたことを特徴とする。

この発明に係る暗号化方法は、暗号化モジュールから出力されるモジュール出力ブロックデータ T_i ($i = 1, 2, 3, \dots$) を用いて第

15 1の平文 M の平文ブロックデータ M_i ($i = 1, 2, 3, \dots$) を暗号化する工程と、

 上記平文ブロックデータ M_i を暗号化している途中で又は平文ブロックデータ M_i を暗号化した後に、第1の平文 M の平文ブロックデータ M_{i+1} の暗号化に用いられるモジュール出力ブロックデータ T_i をメモリ

20 に記憶する工程と、

 上記平文ブロックデータ M_{i+1} の暗号化に用いられるモジュール出力ブロックデータ T_i をメモリに記憶した後に、第2の平文 N の少なくとも1つの平文ブロックデータを暗号化する工程と、

25 上記第2の平文 N の少なくとも1つの平文ブロックデータを暗号化した後に、メモリに記憶された、平文ブロックデータ M_{i+1} の暗号化に用

いられるモジュール出力ブロックデータ T_i を入力し、暗号化モジュールを用いて第 1 の平文 M の平文ブロックデータ M_{i+1} を暗号化する工程と
を備えたことを特徴とする。

5

この発明に係る暗号化装置は、1 つ以上の平文ブロックデータからなる平文を暗号化モジュールにより暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化装置において、

平文ブロックデータを暗号化モジュールにより暗号化したときに暗号
10 化モジュールが出力したモジュール出力ブロックデータ T_i を暗号化モジュールへフィードバックする第 1 のフィードバックループを有し、平文ブロックデータを入力し、第 1 のフィードバックループによりモジュール出力ブロックデータ T_i をフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化部と、

15 認証子演算途中結果をフィードバックする第 2 のフィードバックループを有し、暗号化部から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第 2 のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成部と

20 を備えたことを特徴とする。

上記暗号化部と認証子生成部とは、1 つの暗号化モジュールと、1 つのフィードバックループとを兼用して暗号化処理と認証子生成処理とを交互に行うとともに、

25 上記 1 つのフィードバックループは、
暗号化処理と認証子生成処理との結果をそれぞれ記録し出力するメモ

りと、

暗号化処理と認証生成処理とを交互に実行するために、メモリから暗号化処理と認証子生成処理との結果を交互に選択して暗号化モジュールに出力するセクタと

5 を備えたことを特徴とする。

この発明に係る暗号化方法は、1つ以上の平文ブロックデータからなる平文を暗号化モジュールにより暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化方法において、

10 平文ブロックデータを暗号化モジュールにより暗号化したときに暗号化モジュールが出力したモジュール出力ブロックデータ T_i を暗号化モジュールへフィードバックする第1のフィードバック工程を有し、平文ブロックデータを入力し、第1のフィードバックループによりモジュール出力ブロックデータ T_i をフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化工程と、

15 認証子演算途中結果をフィードバックする第2のフィードバック工程を有し、暗号化工程から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第2のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成工程と

20 を備えたことを特徴とする。

この発明に係る復号装置は、暗号文Cを構成する暗号文ブロックデータ C_i ($i = 1, 2, 3, \dots$) と暗号文Dを構成する暗号文ブロックデータ D_j ($j = 1, 2, 3, \dots$) とを復号する復号装置において、

25

暗号文Cの復号処理中に暗号文Dの復号要求を任意の時点で受け付けるメカニズムと、

復号処理を行ったデータをモジュール出力ブロックデータ T_i として出力する復号モジュールと、

- 5 復号モジュールから出力されたモジュール出力ブロックデータ T_i をフィードバックラインを介し復号モジュールにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記暗号文Dの復号要求を受け付け、暗号文Dのいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号されない場合、フィードバックされるモジュール出力ブロックデータ T_i を記憶するメモリと、

10

暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号される場合は、上記フィードバックループのフィードバックラインによりフィードバックされるモジュール出力ブロックデータ T_i を選択してフィードバックループに供給し、上記暗号文ブロックデータ C_{i+1}

15

が暗号文ブロックデータ C_i の次に続けて復号されず、暗号文Dのいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリに記憶されたモジュール出力ブロックデータ T_i を選択してフィードバックループに供給するセクタと

20

を備えたことを特徴とする。

上記メモリは、

- 25 複数の暗号文に対応した複数のレジスタと、
復号処理をする暗号文に対応してレジスタを切り替えるスイッチと

を備えたことを特徴とする。

この発明に係る復号方法は、復号モジュールから出力されるモジュール出力ブロックデータ T_i ($i = 1, 2, 3, \dots$) を用いて第 1 の暗号文 C の暗号文ブロックデータ C_i ($i = 1, 2, 3, \dots$) を復号する工程と、

上記暗号文ブロックデータ C_i を復号している途中で又は暗号文ブロックデータ C_i を復号した後に、第 1 の暗号文 C の暗号文ブロックデータ C_{i+1} の復号に用いられるモジュール出力ブロックデータ T_i をメモリに記憶する工程と、

上記暗号文ブロックデータ C_{i+1} の復号に用いられるモジュール出力ブロックデータ T_i をメモリに記憶した後に、第 2 の暗号文 D の少なくとも 1 つの暗号文ブロックデータを復号する工程と、

上記第 2 の暗号文 D の少なくとも 1 つの暗号文ブロックデータを復号した後に、メモリに記憶された、暗号文ブロックデータ C_{i+1} の復号に用いられるモジュール出力ブロックデータ T_i を入力し、復号モジュールを用いて第 1 の暗号文 C の暗号文ブロックデータ C_{i+1} を復号する工程と

を備えたことを特徴とする。

20

この発明に係る復号装置は、1 つ以上の暗号文ブロックデータからなる暗号文を復号ユニットにより平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号装置において、

暗号文ブロックデータ C_i を復号ユニットへフィードバックする第 1 のフィードバックループを有し、暗号文ブロックデータを入力し、第 1 のフィードバックループにより暗号文ブロックデータ C_i をフィードバ

25

ックさせ復号処理を行い、平文ブロックデータを出力する復号部と、

- 5 認証子演算途中結果をフィードバックする第2のフィードバックループを有し、復号部に入力される暗号文ブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第2のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成部と
- を備えたことを特徴とする。

- 10 上記復号部と認証子生成部とは、1つの復号モジュールと、1つのフィードバックループとを兼用して復号処理と認証子生成処理とを交互に行うとともに、

- 上記1つのフィードバックループは、
- 復号処理と認証子生成処理との結果をそれぞれ記録し出力するメモリ
- 15 と、

復号処理と認証生成処理とを交互に実行するために、メモリから復号処理と認証子生成処理との結果を交互に選択して復号モジュールに出力するセレクトと

を備えたことを特徴とする。

20

この発明に係る復号方法は、1つ以上の暗号文ブロックデータからなる暗号文を復号ユニットにより平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号方法において、

- 暗号文ブロックデータ C_i を復号ユニットへフィードバックする第1
- 25 のフィードバック工程を有し、暗号文ブロックデータを入力し、第1のフィードバックループにより暗号文ブロックデータ C_i をフィードバック

クさせ復号処理を行い、平文ブロックデータを出力する復号工程と、

認証子演算途中結果をフィードバックする第2のフィードバック工程を有し、復号工程に入力される暗号文ブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し

5、第2のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成工程と

を備えたことを特徴とする。

10 上記暗号化処理は、ブロック暗号アルゴリズムを用いることを特徴とする。

上記復号処理は、ブロック暗号アルゴリズムを用いることを特徴とする。

15

上記メモリは、暗号化処理の状態として、

第1の処理データの暗号化途中結果と、

第1の処理データを暗号化するために用いる暗号鍵とを記憶することを特徴とする。

20

上記メモリは、復号処理の状態として、

第2の処理データの復号途中結果と、

第2の処理データを復号するために用いる復号鍵とを記憶することを特徴とする。

25

この発明に係る暗号化装置は、データを入力して暗号化し、暗号デー

タを出力する暗号化部と、

暗号化部が出力した暗号データを入力して暗号文の完全性を保証するための認証子を生成する認証子生成部とを備え、

- 5 認証子生成部は、暗号化部によるデータの暗号化が完了する前に認証子の生成を開始することを特徴とする。

この発明に係る復号装置は、データを入力して復号し、復号データを出力する復号部と、

- 10 復号部が入力したデータを入力して暗号文の完全性を保証するための認証子を生成する認証子生成部とを備え、

認証子生成部は、復号部によるデータの復号が完了する前に認証子の生成を開始することを特徴とする。

15

この発明に係る暗号化方法は、データを入力して暗号化し、暗号データを出力する暗号化工程と、

暗号化工程が出力した暗号データを入力して暗号文の完全性を保証するための認証子を生成する認証子生成工程と

- 20 を備え、

認証子生成工程は、暗号化工程によるデータの暗号化が完了する前に認証子の生成を開始することを特徴とする。

- 25 この発明に係る復号方法は、データを入力して復号し、復号データを出力する復号工程と、

復号工程が入力したデータを入力して暗号文の完全性を保証するため

の認証子を生成する認証子生成工程と
を備え、

認証子生成工程は、復号工程によるデータの復号が完了する前に認証子の生成を開始することを特徴とする。

5

また、この発明は、上記暗号化装置の各部の処理及び上記暗号化方法の各工程の処理をコンピュータに実行させるためのプログラムであることを特徴とする。また、そのプログラムを記録したコンピュータ読み取り可能な記録媒体であることを特徴とする。

10

また、この発明は、上記復号装置の各部の処理及び上記復号方法の各工程をコンピュータに実行させるためのプログラムであることを特徴とする。また、そのプログラムを記録したコンピュータ読み取り可能な記録媒体であることを特徴とする。

15

図面の簡単な説明

図 1 は、実施の形態 1 の C B C モードの暗号化装置を示す図。

図 2 は、C B C モードの暗号化装置の動作手順を示す図。

図 3 は、C B C モードの暗号化装置の動作フローチャート図。

20

図 4 は、セクタ 5 4 の動作フローチャート図。

図 5 は、スイッチ 5 7 の割り込み処理フローチャート図。

図 6 は、メモリ 5 5 の他の例を示す図。

図 7 は、メモリ 5 5 の割り込み処理フローチャート図。

図 8 は、メモリ 5 5 の他の例を示す図。

25

図 9 は、優先度処理を示す図。

図 1 0 は、優先度処理を示す図。

図 1 1 は、優先度処理を示す図。

図 1 2 は、メモリ 5 5 がフィードバックライン 6 6 と並列に設けられている図。

図 1 3 は、図 1 2 の暗号化装置の動作手順を示す図。

5 図 1 4 は、メモリ 5 5 がフィードバックライン 6 7 に並列に設けられている図。

図 1 5 は、図 1 4 の暗号化装置の動作手順を示す図。

図 1 6 は、O F B モードの暗号化装置を示す図。

図 1 7 は、図 1 6 の暗号化装置の動作手順を示す図。

10 図 1 8 は、C F B モードの暗号化装置を示す図。

図 1 9 は、図 1 8 の暗号化装置の動作手順を示す図。

図 2 0 は、C B C モードの復号装置を示す図。

図 2 1 は、図 2 0 の復号装置の動作手順を示す図。

図 2 2 は、O F B モードの復号装置を示す図。

15 図 2 3 は、図 2 2 の復号装置の動作手順を示す図。

図 2 4 は、C F B モードの復号装置を示す図。

図 2 5 は、図 2 4 の復号装置の動作手順を示す図。

図 2 6 は、鍵を保存する C B C モードの暗号化装置を示す図。

図 2 7 は、C B C モードの暗号化装置の動作手順を示す図。

20 図 2 8 は、鍵を保存する C B C モードの復号装置を示す図。

図 2 9 は、実施の形態 2 の暗号化部 1 0 0 と認証子生成部 2 0 0 を有する暗号化装置を示す図。

図 3 0 は、暗号化部 1 0 0 と認証子生成部 2 0 0 を有する暗号化装置の動作手順を示す図。

25 図 3 1 は、暗号化部 1 0 0 と認証子生成部 2 0 0 を有する暗号化装置のフローチャート図。

図 3 2 は、暗号化部 1 0 0 と認証子生成部 2 0 0 を 1 つにした暗号化装置を示す図。

図 3 3 は、暗号化部 1 0 0 と認証子生成部 2 0 0 を 1 つにした暗号化装置の動作手順を示す図。

5 図 3 4 は、復号化部 3 0 0 と認証子生成部 4 0 0 を有する復号装置を示す図。

図 3 5 は、復号化部 3 0 0 と認証子生成部 4 0 0 を 1 つにした復号装置を示す図。

10 図 3 6 は、復号化部 3 0 0 と認証子生成部 4 0 0 を 1 つにした復号装置の動作手順を示す図。

図 3 7 は、実施の形態 2 の暗号化部 1 0 0 と認証子生成部 2 0 0 を有する暗号化装置を示す図。

図 3 8 は、復号化部 3 0 0 と認証子生成部 4 0 0 を有する復号装置を示す図。

15 図 3 9 は、暗号鍵 K を用いた暗号化モジュール 5 1 の代表的構成図。

図 4 0 は、暗号化装置及び復号装置のハードウェア実現例を示す図。

図 4 1 は、暗号化装置及び復号装置のハードウェア実現例を示す図。

図 4 2 は、アプリケーションプログラム 4 6 により暗号化プログラム 4 7 が呼び出される場合を示す図。

20 図 4 3 は、従来の C B C モードの暗号化装置を示す図。

図 4 4 は、従来の C B C モードによる復号装置を示す図。

図 4 5 は、従来の O F B モードの暗号化装置を示す図。

図 4 6 は、従来の O F B モードによる復号装置を示す図。

図 4 7 は、従来の C F B モードの暗号化装置を示す図。

25 図 4 8 は、従来の C F B モードによる復号装置を示す図。

図 4 9 は、従来の暗号化手順を示す図。

図 5 0 は、従来の暗号化手順を示す図。

図 5 1 は、秘匿処理と完全性保証処理を説明する図。

図 5 2 は、従来の秘匿処理と完全性保証処理の動作手順を示す図。

5 発明を実施するための最良の形態

実施の形態 1.

図 1 は、この実施の形態における C B C モードの暗号化装置を示す図である。

この実施の形態の暗号化装置は、セクタ 5 4 と排他的論理和回路 5 8 と暗号鍵 K を用いた暗号化モジュール 5 1 とメモリ 5 5 とにより構成されている。排他的論理和回路 5 8 と暗号鍵 K を用いた暗号化モジュール 5 1 とは、暗号化ユニット 5 2 を構成している。セクタ 5 4 と排他的論理和回路 5 8 と暗号鍵 K を用いた暗号化モジュール 5 1 は、フィードバックライン 6 5 とフィードバックライン 6 6 とフィードバックライン 6 7 によりフィードバックループを構成している。暗号鍵 K を用いた暗号化モジュール 5 1 により暗号化された暗号文ブロックデータ C_i は、フィードバックループにより再び排他的論理和回路 5 8 に入力され、排他的論理和回路 5 8 でモジュール入力データ S_i が生成される。そして、生成されたモジュール入力データ S_i が暗号鍵 K を用いた暗号化モジュール 5 1 に供給される。

メモリ 5 5 は、フィードバックライン 6 5 と並列に設けられている。メモリ 5 5 は、レジスタ 5 6 とスイッチ 5 7 により構成されている。スイッチ 5 7 は、暗号鍵 K を用いた暗号化モジュール 5 1 の出力をレジスタ 5 6 に入力させるか無視するかを切り替えるものである。この切り替えは、例えば、割り込み I T により行われる。割り込み I T が発生した場合には、スイッチ 5 7 は E に接続され、割り込み I T が解除された場

合には、スイッチ 5 7 は F に接続される。レジスタ 5 6 は、E を経由してきた暗号文ブロックデータ C_i を入力して記憶するものである。レジスタ 5 6 に記憶された暗号文ブロックデータ C_i は、セクタ 5 4 に出力される。セクタ 5 4 は、A, B, C の 3 つの入力を有しており、い
5 ずれか 1 つの入力を選択するものである。これらの選択は、後述するように割り込み I T に依存する。

図 2 は、図 1 に示した暗号化装置の動作手順を示す図である。

図 3 は、図 1 に示した暗号化装置の動作フローチャートである。

この暗号化装置が電源を投入された場合のセクタ 5 4 の入力は A に
10 設定されており、スイッチ 5 7 は E に接続されているものとする。また、平文 N の暗号化要求があるときは、割り込み I T が発生し、平文 N の暗号化要求が解除されるまで、割り込み I T がオンになり続けるものとする。また、平文 M は、鍵 K_1 を用いて暗号化され、平文 N は、鍵 K_2 を用いて暗号化されるものとする。また、割り込み I T が発生したとき
15 又は割り込み I T が解除されたときには、鍵 K_2 又は鍵 K_1 が暗号化モジュール 5 1 に支給され直すものとする。

時刻 T 0 において、鍵 K_1 が支給され、平文ブロックデータ M_1 の暗号化処理がスタートする。時刻 T 0 において、平文ブロックデータ M_1 の暗号化がスタートした場合には、セクタ 5 4 の入力 A から一旦イン
20 シタルバリュウ I V が入力された後、セクタ 5 4 は B に切り替わる。そして、平文ブロックデータ M_1 が鍵 K_1 を用いて暗号化されている途中の時刻 X において、平文ブロックデータ N_1 の暗号化を要求する割り込み I T が発生したとする。時刻 T 1 までに、暗号文ブロックデータ C_1 はメモリ 5 5 に記憶された状態になる。そして、割り込み I T の発生
25 により時刻 T 1 において、鍵 K_2 が暗号化モジュール 5 1 に支給される。また、時刻 T 1 において、セクタ 5 4 は入力を A に設定する。また

、時刻 T_1 において、スイッチ 57 は F に接続される。時刻 T_1 以降は、鍵 K_2 を用いて平文ブロックデータ N_1 の暗号化が行われ、暗号文ブロックデータ D_1 が出力される。時刻 Y において、平文ブロックデータ N_1 の暗号化が終了し、割り込み IT が解除されたものとする。この割り込み IT の解除により時刻 T_2 において、鍵 K_1 が暗号化モジュール 51 に支給され、セクタ 54 の入力 は C に切り替えられ、スイッチ 57 は E に接続される。セクタ 54 が C に切り替わったことにより、メモリ 55 に記憶されていた暗号文ブロックデータ C_1 が平文ブロックデータ M_2 の暗号化のために入力され、鍵 K_1 を用いた暗号化モジュール 51 により平文ブロックデータ M_2 が暗号化されて、暗号文ブロックデータ C_2 が出力される。時刻 T_3 以前においては、セクタ 54 の入力 は B に切り替えられ、平文ブロックデータ M_3 を暗号化する場合には、フィードバックループのフィードバックライン 65 からフィードバックされた暗号文ブロックデータ C_2 が入力され、鍵 K_1 を用いた暗号化モジュール 51 により平文ブロックデータ M_3 暗号化されて、暗号文ブロックデータ C_3 が出力される。

なお、平文 M と平文 N の鍵が同一 ($K_1 = K_2$) の場合は、鍵は暗号処理のスタート時に一度だけ供給されればよい。

図 3 のフローチャートを用いて全体の動作を説明する。

S 1 において、平文 M の暗号化処理がスタートし続行される。最後のブロックデータまで処理を終えた場合には、処理を終了する。S 2 において、任意の時点で生じる割り込み IT の発生が監視される。割り込み IT の発生がない場合には、S 1 の処理が続行される。平文ブロックデータ M_i の処理中に割り込み IT が発生した場合には、S 3 において、現在処理中の平文ブロックデータ M_i の暗号文ブロックデータ C_i をメモリ 55 のレジスタ 56 に記憶する。S 4 において、割り込み IT によ

り暗号化処理の要求があった平文Nの暗号化処理を行う。このS 4の暗号化処理は、S 5に示すように、割り込みITの解除があるまで連続して行われる。割り込みITの解除があった場合には、S 6において、メモリ55のレジスタ56に記憶した暗号文ブロックデータ C_i を用いて

5 M_{i+1} の暗号化処理を行う。それ以降の処理は、S 1に戻り、暗号化処理が続行される。

図4は、セクタ54のオペレーション処理を示す図である。

電源がオンになった場合には、S 11に示すように、入力をAに設定する。S 12において、暗号化がスタートした場合には、S 13において、

10 入力をBに設定する。即ち、フィードバックループのフィードバックライン65によりフィードバックされる暗号文ブロックデータ C_i が用いられる。S 14において、現在処理しているブロックデータが最後であるということが判定された場合には、S 11に戻り電源オンと同じ状態に戻る。S 15において、割り込みITの発生が確認された場合には、

15 S 16において、入力をAに設定し、暗号化がスタートした場合には、S 18において、入力をBに設定する。割り込みITの解除があるまでは、入力がBに設定されたままで動作する。即ち、フィードバックループのフィードバックライン65によりフィードバックされる暗号文ブロックデータ C_i が用いられる。S 19において、割り込みITの解

20 除があったことが検知された場合には、S 20において、入力をCに設定する。この入力をCに設定することにより、メモリ55に記憶された暗号文ブロックデータ C_i が入力されることになる。このCからの入力による暗号化がスタートした場合には、S 13に戻り入力をBに設定する。

25 このようにして、割り込みITの発生に基づき、セクタ54を切り替えることができる。

なお、平文Mの暗号化処理も、割り込みITにより任意の時刻にスタートさせてもよい。

図5は、スイッチ57の割り込み処理のフローチャートである。

電源がオンになった場合、そして、その後の最初の平文の暗号化処理
5 の場合は、スイッチ57はEに接続される。そして、S31において、
割り込みITが発生した場合には、スイッチ57をEからFに接続する。
そして、S33において、割り込みITの解除が検出された場合には、
スイッチ57をFからEに接続する。このようにして、スイッチ57
は、割り込みITの発生から解除までは暗号文ブロックデータ C_i を無
10 視する。従って、メモリ55のレジスタ56には、割り込みITが発生
したときに生成された暗号文ブロックデータ C_i が記憶され続けること
になる。

以上のように、図1～図5に示した暗号化装置は、平文Mを構成する
平文ブロックデータ M_i ($i = 1, 2, 3, \dots$)と平文Nを構成す
15 る平文ブロックデータ N_j ($j = 1, 2, 3, \dots$)とを暗号化する
暗号化装置において、平文Mの暗号化処理中に平文Nの暗号化要求を平
文Mの暗号化処理完了前に受け付ける割り込み処理メカニズムを示して
いる。

また、図1～図5に示した暗号化装置は、平文ブロックデータ M_i の
20 暗号化処理を行い、暗号文ブロックデータ C_i を出力する暗号化モジュ
ール51と、暗号化モジュール51から出力された暗号文ブロックデー
タ C_i をフィードバックライン65を介し暗号化ユニット52にフィー
ドバックするフィードバックループ65、66と、フィードバックルー
プのフィードバックライン65と並列に設けられ、上記割り込み処理に
25 より上記平文Nの暗号化要求を受け付け、平文Nのいずれかの平文ブ
ロックデータの暗号化処理を開始することにより、上記平文ブロックデー

タ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化されない場合、フィードバックされる暗号文ブロックデータ C_i を記憶するメモリ 55 とを有している。

また、図 1 ～図 5 に示した暗号化装置は、平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化される場合は、上記フィードバックループのフィードバックライン 65 によりフィードバックされる暗号文ブロックデータ C_i を選択してフィードバックループを介して暗号化ユニット 52 に供給し、上記平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化されず、平文 N のいずれかの平文ブロックデータの次に暗号化される場合は、上記メモリ 55 に記憶された暗号文ブロックデータ C_i を選択してフィードバックループを介して暗号化ユニット 52 に供給するセクタ 54 を有している。

メモリ 55 は、割り込み IT が発生したときの暗号化装置の状態を記憶するメモリである。メモリ 55 が暗号化処理の状態を記憶しておくことにより、あるデータの暗号化の最中に他のデータの暗号化を行った場合でも、再びあるデータの暗号化の処理に復帰することができる。即ち、メモリ 55 に記憶されたデータを用いることにより、暗号化が中断されたときと全く同じ状態に暗号化装置を復帰させることができ、中断した暗号化処理を続行させることが可能になる。

図 6 は、メモリ 55 の他の例を示す図である。

メモリ 55 は、割り込み制御部 52 と入力スイッチ 96 と出力スイッチ 97 と複数のレジスタ (REG 1, 2, 3) を有している。このように、複数のレジスタを有することにより、複数の割り込みを受け付けることが可能になる。

図 7 は、メモリ 55 の割り込み処理の動作を示す図である。

割り込み IT が発生すると、S 41において、現在使用中のレジスタ

kの番号kを記憶する。S 4 2において、入力スイッチ9 6と出力スイッチ9 7をレジスタk以外のレジスタlに接続する。この状態で、平文Nの暗号化が継続される。更に、平文Nの暗号化の最中に他の割り込みが発生したかを監視する。S 4 3において、他の割り込みI Tが発生したことが検出された場合には、再び自分自身であるS 4 0の処理を呼び出す。このように、割り込みI Tが発生するたびに、自分自身をS 4 0の処理をリカーシブに呼び出すことにより、複数階層の割り込み処理を行うことができる。S 4 4においては、割り込みが解除されたかを検出し、割り込みが解除された場合には、入力スイッチ9 6と出力スイッチ9 7を記憶しておいた番号kを用いてレジスタkに切り替える。図6に示す場合は、3つのレジスタがあるので、3階層の割り込み処理を行うことができる。

図8は、メモリ5 5の他の例を示す図である。

メモリ5 5は、スタック6 4を有している。スタック6 4は、先入れ後出し（F I L O）のレジスタである。スタック1を使用中に割り込みI Tが発生した場合には、スタック1のデータをスタック2に移し、それ以後のデータをスタック1に積み上げ、割り込みI Tが解除された場合には、積み上げたスタック1のデータを出力し、スタック2のデータをスタック1に戻す。図8に示す場合は、4階層の割り込み処理を行える場合を示している。

図6に示すように、複数階層の割り込み処理を行うことができる場合は、各割り込みに対して優先度を付けることができる。例えば、割り込みI T 1を優先度1とし、割り込みI T 2を優先度1より優先度の低い優先度2とすることにより、優先度1の割り込みI T 1が発生した場合には、優先度2の処理を遅らせることができる。

図9は、優先度1の暗号化処理を優先度2の暗号化処理に優先させた

場合を示している。優先度 1 の暗号化処理を先に終了させている。

図 10 は、優先度がともに等しい場合の暗号化処理の場合を示している。

優先度が等しい場合には、2 つの平文の各ブロックデータを交互に暗
5 号化する。

図 11 は、優先度 1 のデータと 2 つの優先度 2 のデータを暗号化する
場合を示している。

図 9 ～図 11 に示すように、割り込みに優先度を付けることによりユ
ーザが望ましいと思われる暗号化処理手順を実現することができる。緊
10 急用のデータや短いデータの場合には、優先度を高くすることにより効
率のよい処理を行うことができる。

図 12 は、メモリ 55 をフィードバックライン 66 と並列においた場
合を示している。

排他的論理和回路 58 と暗号鍵 K を用いた暗号化モジュール 51 とは
15 、暗号化ユニット 52 を構成している。

図 13 は、図 12 の暗号化装置の動作手順を示す図である。

第 1 セレクタ 61 と第 2 セレクタ 62 とは、以下のような選択接続に
より、図 1 のセレクタ 54 と同じ選択動作をさせるものである。

第 1 のセレクタ 61 + 第 2 のセレクタ 62 = セレクタ 54

20	A	+	D	=	A
	B	+	D	=	B
	A	+	C	=	C
	B	+	C	=	C

図 13 では、第 2 のセレクタ 62 が D を選択しているときは、第 1 の
25 セレクタ 61 の選択 (A 又は B) が有効となり、第 2 のセレクタ 62 が
C を選択しているときは、メモリ 55 の内容が出力されることになる。

即ち、第2のセクタ62は、メモリ55の内容を用いたいとき（割り込みITが解除されて平文Nから元の平文Mへの暗号化に戻るとき）に、Cを選択すればよい。

図14は、メモリ55をフィードバックライン67と並列においた場合を示している。

図15は、図14の暗号化装置の動作手順を示す図である。

割り込みITが発生した時刻Xが排他的論理和回路58で排他的論理和演算される前である場合には、メモリ55は、排他的論理和回路58により排他的論理和演算されたモジュール入力データ S_i を記憶する。

そして、平文ブロックデータ N_i を暗号化する。次に、メモリ55に記憶されたモジュール入力データ S_i を第2セクタ62により選択させ、暗号鍵Kを用いた暗号化モジュール51に入力し、暗号化して暗号文ブロックデータ C_i を出力する。

図1及び図12及び図14に示すように、メモリ55は、フィードバックライン65とフィードバックライン66とフィードバックライン67のいずれのラインと並列の設けられていても構わない。メモリ55は、暗号化装置が、あるデータの暗号化処理中に他のデータの暗号化を開始するとき、他のデータの暗号化を開始する直前の状態を覚えておくものであり、他のデータの暗号化処理が終了した時点で、メモリ55に記憶されたデータを用いて暗号化装置が元の状態に復帰できるのであれば、メモリ55は、どの場所に設けられていても構わない。また、メモリ55は、複数箇所に設けられていてもよい。

以上のように、この実施の形態に係る暗号化装置は、1つ以上のブロックデータ M_i ($i = 1, 2, 3, \dots, m$) からなる第1の処理データ（平文M）と、1つ以上のブロックデータ N_j ($j = 1, 2, 3, \dots, n$) からなる第2の処理データ（平文N）との暗号化処理をす

る暗号化装置において、暗号化処理の状態を記憶するメモリ 55 を備え、第 1 の処理データの全ブロックデータ ($M_1 \sim M_n$) の暗号化処理が完了する前に第 2 の処理データの最初のブロックデータ N_1 の暗号化処理を開始するとともに、第 2 の処理データの最初のブロックデータ N_1 の暗号化処理を開始する場合に第 1 の処理データの暗号化処理の状態（例えば、暗号化ブロックデータ C_i ）を上記メモリ 55 に記憶させ、第 1 の処理データの暗号化処理を再開する場合に、暗号化装置の暗号化処理の状態を、メモリに記憶した第 1 の処理データの暗号化処理の状態に復帰させてから第 1 の処理データの暗号化処理を再開することを特徴とする。

また、上記暗号化装置は、第 2 の処理データの全ブロックデータ ($N_1 \sim N_n$) の暗号化処理の完了する前に第 1 の処理データの暗号化処理を再開するとともに、上記メモリ 55 は、第 1 の処理データの暗号化処理を再開する場合に第 2 の処理データの暗号化処理状態（例えば、暗号化ブロックデータ D_j ）を記憶し、第 2 の処理データの暗号化処理を再開する場合は、暗号化装置の暗号化処理の状態を、メモリに記憶した第 2 の処理データの暗号化処理の状態に復帰させてから第 2 の処理データの暗号化処理を再開することを特徴とする。

図 16 は、OFB モードの暗号化装置の構成図である。

図 45 に比べて、メモリ 55 が追加されている点が特徴である。メモリ 55 は、暗号化モジュール 51 から出力されたモジュール出力データ T_1 を記憶するものである。

図 16 は、平文 M を構成する平文ブロックデータ M_i ($i = 1, 2, 3, \dots$) と平文 N を構成する平文ブロックデータ N_j ($j = 1, 2, 3, \dots$) とを暗号化する暗号化装置において、平文 M の暗号化処理中に平文 N の暗号化要求を平文 M の暗号化処理完了前に受け付ける割

り込み処理メカニズムと、暗号化処理を行ったデータをモジュール出力
ブロックデータ T_i として出力する暗号化モジュール51と、暗号化モ
ジュール51から出力されたモジュール出力ブロックデータ T_i をフィ
ードバックライン65を介し暗号化モジュールにフィードバックするフ
ードバックループ65、66と、フィードバックループのフィードバ
ックライン65と並列に設けられ、上記平文 N の暗号化要求を受け付け
、平文 N のいずれかの平文ブロックデータの暗号化処理を開始すること
により、上記平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次
に続けて暗号化されない場合、フィードバックされるモジュール出力ブ
ロックデータ T_i を記憶するメモリ55と、平文ブロックデータ M_{i+1}
が平文ブロックデータ M_i の次に続けて暗号化される場合は、上記フィ
ードバックループのフィードバックライン65によりフィードバックさ
れるモジュール出力ブロックデータ T_i を選択してフィードバックルー
プを介して暗号化モジュール51に供給し、上記平文ブロックデータ M_{i+1}
が平文ブロックデータ M_i の次に続けて暗号化されず、平文 N のい
ずれかの平文ブロックデータの次に暗号化される場合は、上記メモリ5
5に記憶されたモジュール出力ブロックデータ T_i を選択してフィード
バックループを介して暗号化モジュール51に供給するセクタ54と
を備えたことを特徴とする。

図17は、図16のOFBモードの暗号化装置の動作説明図である。

図17は、図2のCBCモードの動作がOFBモードの動作になった
ものであり、その他の動作は図2の動作と同じである。

図18は、CFBモードの暗号化装置を示す図である。

図47に比べて、メモリ55が設けられている点が特徴である。メモ
リ55は、排他的論理和回路58から出力された暗号文ブロックデータ
 C_i を記憶するものである。

また、排他的論理和回路 5 8 と暗号鍵 K を用いた暗号化モジュール 5 1 とは、暗号化ユニット 5 2 を構成している。

図 1 8 は、平文 M を構成する平文ブロックデータ M_i ($i = 1, 2, 3, \dots$) と平文 N を構成する平文ブロックデータ N_j ($j = 1, 2, 3, \dots$) とを暗号化する暗号化装置において、平文 M の暗号化処理中に平文 N の暗号化要求を平文 M の暗号化処理完了前に受け付ける割り込み処理メカニズムと、平文ブロックデータ M_i の暗号化処理を行い暗号文ブロックデータ C_i を出力する暗号化ユニット 5 2 と、暗号化モジュールから出力された暗号文ブロックデータ C_i をフィードバックライン 6 5 を介し暗号化処理にフィードバックするフィードバックループ 6 5, 6 6 と、フィードバックループのフィードバックライン 6 5 と並列に設けられ、上記平文 N の暗号化要求を受け付け、平文 N のいずれかの平文ブロックデータの暗号化処理を開始することにより、上記平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化されない場合、フィードバックされる暗号文ブロックデータ C_i を記憶するメモリ 5 5 と、平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化される場合は、上記フィードバックループのフィードバックライン 6 5 によりフィードバックされる暗号文ブロックデータ C_i を選択してフィードバックループを介して暗号化ユニット 5 2 に供給し、上記平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化されず、平文 N のいずれかの平文ブロックデータの次に暗号化される場合は、上記メモリ 5 5 に記憶された暗号文ブロックデータ C_i を選択してフィードバックループを介して暗号化ユニット 5 2 に供給するセレクタ 5 4 とを備えたことを特徴とする。

図 1 9 は、図 1 8 の C F B モードの暗号化装置の動作説明図である。

図 1 9 は、図 2 の C B C モードの動作が C F B モードの動作になった

ものであり、その他の動作は図 2 の動作と同じである。

図 20 は、CBC モードの復号装置を示す図である。

図 44 に比べて、メモリ 75 が設けられている点が特徴である。

メモリ 75 は、レジスタ 76 とスイッチ 77 により構成されている。

- 5 また、排他的論理和回路 78 と鍵 K を用いた復号モジュール 71 により復号ユニット 72 を構成している。

なお、レジスタ 111 は、セクタ 74 の内部に設けられていてもよい。

- 図 20 に示す復号装置は、暗号文 C を構成する暗号文ブロックデータ
10 C_i ($i = 1, 2, 3, \dots$) と暗号文 D を構成する暗号文ブロックデータ N_j ($j = 1, 2, 3, \dots$) とを復号する復号装置において、暗号文 C の復号処理中に暗号文 D の復号要求を任意の時点で受け付ける割り込み処理メカニズムを有している。

- また、図 20 に示す復号装置は、暗号文ブロックデータ C_i の復号処理
15 を行ったデータをモジュール出力ブロックデータ T_i として出力する復号モジュール 71 と、暗号文ブロックデータ C_{i+1} を復号するための暗号文ブロックデータ C_i をフィードバックライン 85, 111, 82 を介し復号ユニット 72 にフィードバックするフィードバックループ 85, 111, 82, 86 と、フィードバックループのフィードバックライン 85, 111, 82 と並列に設けられ、上記暗号文 D の復号要求を受け付け、暗号文 D のいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号されない場合、フィードバックされるブロックデータを記憶するメモリ 71 とを有している。

- 25 また、図 20 に示す復号装置は、暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号される場合は、上記フィードバ

ックループのフィードバックライン 85, 111, 82によりフィードバックされる暗号文ブロックデータ C_i を選択してフィードバックループを介して暗号ユニット 72 に供給し、上記暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号されず、暗号文 D のいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリに記憶された暗号文ブロックデータ C_i を選択してフィードバックループを介して暗号ユニット 72 に供給するセクタ 74 を備えている。

なお、上述した図 20 の説明において、「フィードバックライン」、「フィードバックループ」という用語を用いているが、「自己の出力を自己の入力にする」という意味での「フィードバック」ではない。ここでは、「フィードバック」という用語は、暗号文ブロックデータ C_i を復号した後に、暗号文ブロックデータ C_{i+1} を復号するために、暗号文ブロックデータ C_i を再び供給するという意味で用いるものとする。

図 21 は、図 20 の復号装置の動作手順を示す図である。

暗号鍵（復号鍵ともいう） K_1 を用いて、暗号文ブロックデータ C_1 を復号している最中に割り込み IT の発生があった場合には、暗号文ブロックデータ C_1 がメモリ 75 のレジスタ 76 に記憶される。その後、暗号鍵（復号鍵ともいう） K_2 を用いて、暗号文ブロックデータ D_1 の復号が行われ、平文ブロックデータ N_1 が復号される。そして、メモリ 75 のレジスタ 76 に記憶された暗号文ブロックデータ C_1 が読み出され、暗号文ブロックデータ C_2 の復号が行われ、平文ブロックデータ M_2 が復号される。セクタ 74 の動作は、図 4 に示したものと同一である。また、スイッチ 77 の動作は、図 5 に示したものと同一である。

図 22 は、OFB モードの復号装置を示す図である。

図 22 は、暗号文 C を構成する暗号文ブロックデータ C_i ($i = 1, 2, 3, \dots$) と暗号文 D を構成する暗号文ブロックデータ D_j (j

$= 1, 2, 3, \dots$) とを復号する復号装置において、暗号文 C の復号処理中に暗号文 D の復号要求を任意の時点で受け付ける割り込み処理メカニズムと、復号処理を行ったデータをモジュール出力ブロックデータ T_i として出力する復号モジュール 71 と、復号モジュール 71 から

5 出力されたモジュール出力ブロックデータ T_i をフィードバックライン 85 を介し復号モジュール 71 にフィードバックするフィードバックループ 85, 86 と、フィードバックループのフィードバックライン 85 と並列に設けられ、上記暗号文 D の復号要求を受け付け、暗号文 D のいずれかの暗号文ブロックデータの復号処理を開始することにより、上記

10 暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号されない場合、フィードバックされるモジュール出力ブロックデータ T_i を記憶するメモリ 75 と、暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号される場合は、上記フィードバックループのフィードバックライン 85 によりフィードバックされるモジ

15 ュール出力ブロックデータ T_i を選択してフィードバックループを介して復号モジュール 71 に供給し、上記暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号されず、暗号文 D のいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリ 75 に記憶されたモジュール出力ブロックデータ T_i を選択してフィードバック

20 ループを介して復号モジュール 71 に供給するセレクタ 74 とを備えたことを特徴とする。

図 23 は、図 22 の OFB モードの暗号化装置の動作説明図である。

図 23 は、図 21 の CBC モードの動作が OFB モードの動作になったものであり、その他の動作は図 21 の動作と同じである。

25 図 24 は、CFB モードの復号装置を示す図である。

また、排他的論理和回路 78 と鍵 K を用いた復号モジュール 71 によ

り復号ユニット 7 2 を構成している。

なお、レジスタ 1 1 1 は、セクタ 7 4 の内部に設けられていてもよい。

図 2 4 は、暗号文 C を構成する暗号文ブロックデータ C_i ($i = 1, 2, 3, \dots$) と暗号文 D を構成する暗号文ブロックデータ D_j ($j = 1, 2, 3, \dots$) とを復号する復号装置において、暗号文 C の復号処理中に暗号文 D の復号要求を任意の時点で受け付ける割り込み処理メカニズムと、暗号文ブロックデータ C_i の復号処理を行ったデータをモジュール出力ブロックデータ T_i として出力する復号モジュール 7 1 と、暗号文ブロックデータ C_{i+1} を復号するための暗号文ブロックデータ C_i をフィードバックライン 8 5, 1 1 1, 8 2 を介し復号ユニット 7 2 にフィードバックするフィードバックループ 8 5, 1 1 1, 8 2, 8 6 と、フィードバックループのフィードバックライン 8 5, 1 1 1, 8 2 と並列に設けられ、上記暗号文 D の復号要求を受け付け、暗号文 D のいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号されない場合、フィードバックされる暗号文ブロックデータ C_i を記憶するメモリ 7 5 と、暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号される場合は、上記フィードバックループのフィードバックライン 8 5, 1 1 1, 8 2 によりフィードバックされる暗号文ブロックデータ C_i を選択してフィードバックループを介して復号モジュール 7 1 に供給し、上記暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号されず、暗号文 D のいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリ 7 5 に記憶された暗号文ブロックデータ C_i を選択してフィードバックループを介して復号モジュール 7 1 に供給するセクタ 7 4 とを備えたことを

特徴とする。

なお、上述した図 2 4 の説明において、「フィードバックライン」、「フィードバックループ」という用語を用いているが、「自己の出力を自己の入力にする」という意味での「フィードバック」ではない。ここでは、「フィードバック」という用語は、暗号文ブロックデータ C_i を復号した後に、暗号文ブロックデータ C_{i+1} を復号するために、暗号文ブロックデータ C_i を再び供給するという意味で用いるものとする。

図 2 5 は、図 2 4 の C F B モードの暗号化装置の動作説明図である。

図 2 5 は、図 2 1 の C B C モードの動作が C F B モードの動作になったものであり、その他の動作は図 2 1 の動作と同じである。

図 2 6 は、図 1 に示した C B C モードの暗号化装置の改良例を示す図である。

図 2 6 の暗号化装置は、セクタ 1 5 4 とメモリ 1 5 5 とが追加されている。図 1 の場合は、鍵 K_1 が割り込み I T の解除のとき外部から支給される場合を示したが、ここでは、一度外部から支給された鍵 K_1 を保存して再利用する場合について説明する。

メモリ 1 5 5 は、レジスタ 1 5 6 とスイッチ 1 5 7 により構成されている。スイッチ 1 5 7 は、暗号鍵 K をレジスタ 1 5 6 に入力させるか無視するかを切り替えるものである。この切り替えは、例えば、割り込み I T により行われる。割り込み I T が発生した場合には、スイッチ 1 5 7 は E に接続され、割り込み I T が解除された場合には、スイッチ 1 5 7 は F に接続される。レジスタ 1 5 6 は、E を経由してきた鍵 K を入力して記憶するものである。レジスタ 1 5 6 に記憶された鍵 K は、セクタ 1 5 4 に出力される。セクタ 1 5 4 は、A、C の 2 つの入力を有しており、いずれか 1 つの入力を選択するものである。これらの選択は、後述するように割り込み I T に依存する。

図 27 は、図 26 に示した暗号化装置の動作手順を示す図である。

この暗号化装置が電源を投入された場合のセクタ 54 とセクタ 154 の入力 A に設定されており、スイッチ 57 とスイッチ 157 は E に接続されているものとする。また、平文 N の暗号化要求があるときは、
5 割り込み IT が発生し、平文 N の暗号化要求が解除されるまで、割り込み IT がオンになり続けるものとする。また、平文 M は、鍵 K_1 を用いて暗号化され、平文 N は、鍵 K_2 を用いて暗号化されるものとする。鍵 K_1 又は鍵 K_2 が暗号化モジュール 51 に支給されるものとする。

時刻 T0 において、鍵 K_1 が鍵 KI として外部から支給される。セクタ 154 は、A に接続されているので、鍵 KI を鍵 K として暗号化モジュール 51 に出力する。また、スイッチ 157 が E に接続されているので、鍵 K_1 がレジスタ 156 に記憶される。そして、平文ブロックデータ M_1 の暗号化処理がスタートする。時刻 T0 において、平文ブロックデータ M_1 の暗号化がスタートした場合には、セクタ 54 の入力 A から一旦イニシャルバリュー IV が入力された後、セクタ 54 は B に切り替わる。そして、平文ブロックデータ M_1 が鍵 K_1 を用いて暗号化されている途中の時刻 X において、平文ブロックデータ N_1 の暗号化を要求する割り込み IT が発生したとする。時刻 T1 までに、暗号文ブロックデータ C_1 はメモリ 55 に記憶された状態になる。そして、割り込み IT の発生により時刻 T1 において、鍵 K_2 が鍵 KI として外部から暗号化モジュール 51 に支給される。セクタ 154 は、A に接続されているので、鍵 KI を鍵 K として暗号化モジュール 51 に出力する。また、時刻 T1 において、セクタ 54 は入力を A に設定する。また、時刻 T1 において、スイッチ 57 とスイッチ 157 は F に接続される。従って、鍵 K_2 は、レジスタ 156 に記憶されない。時刻 T1 以降は、鍵 K_2 を用いて平文ブロックデータ N_1 の暗号化が行われ、暗号文ブロッ

クデータ D_1 が出力される。時刻 Y において、平文ブロックデータ N_1 の暗号化が終了し、割り込み $I\ T$ が解除されたものとする。この割り込み $I\ T$ の解除により時刻 $T\ 2$ において、セクタ $5\ 4$ の入力は C に切り替えられ、スイッチ $5\ 7$ は E に接続される。従って、鍵 K_1 がレジスタ

5 $1\ 5\ 6$ から鍵 $K\ I$ としてセクタ $1\ 5\ 4$ に出力され、セクタ $1\ 5\ 4$ から鍵 K_1 が鍵 K として暗号化モジュール $5\ 1$ に支給される。また、セクタ $5\ 4$ が C に切り替わったことにより、メモリ $5\ 5$ に記憶されていた暗号文ブロックデータ C_1 が平文ブロックデータ M_2 の暗号化のために

10 入力され、鍵 K_1 を用いた暗号化モジュール $5\ 1$ により平文ブロックデータ M_2 が暗号化されて、暗号文ブロックデータ C_2 が出力される。時刻 $T\ 3$ 以前においては、セクタ $5\ 4$ の入力は B に切り替えられ、平文ブロックデータ M_3 を暗号化する場合には、フィードバックループのフィードバックライン $6\ 5$ からフィードバックされた暗号文ブロックデータ C_2 が入力され、鍵 K_1 を用いた暗号化モジュール $5\ 1$ により平文ブ

15 ロックデータ M_3 が暗号化されて、暗号文ブロックデータ C_3 が出力される。

また、時刻 $T\ 3$ 以前においては、セクタ $1\ 5\ 4$ の入力は、 A に切り替えられる。

セクタ $1\ 5\ 4$ のオペレーション処理を説明する。

20 電源がオンになった場合には、入力を A に設定する。また、割り込み $I\ T$ の発生が確認された場合でも、入力を A に設定し続ける。割り込み $I\ T$ の解除があるまでは、セクタ $1\ 5\ 4$ は、入力が A に設定されたままで動作する。セクタ $1\ 5\ 4$ は、割り込み $I\ T$ の解除があったことが検知された場合に、入力を C に設定する。この入力を C に設定すること

25 により、メモリ $5\ 5$ に記憶された鍵 K_1 が鍵 K として暗号化モジュール $5\ 1$ に入力されることになる。この C からの鍵入力による暗号化がスタ

ートした場合には、セクタ 1 5 4 は、入力を A に設定する。

このようにして、割り込み I T の発生に基づき、セクタ 1 5 4 を切り替えることができる。

次に、スイッチ 1 5 7 の割り込み処理のオペレーションを説明する。

- 5 電源がオンになった場合、そして、その後の最初の平文 M の暗号化処理の場合は、スイッチ 1 5 7 は E に接続され、平文 M の鍵 K_1 がレジスタ 1 5 6 に記憶される。そして、時刻 X にて、割り込み I T が発生した場合には、時刻 T_1 でスイッチ 1 5 7 を E から F に接続し、平文 N の鍵 K_2 を無視する。そして、時刻 Y にて、割り込み I T の解除が検出された場合には、時刻 T_2 にて、スイッチ 1 5 7 を F から E に接続する。このようにして、スイッチ 1 5 7 は、割り込み I T の発生から解除までは平文 N の鍵 K_2 を無視する。従って、メモリ 1 5 5 のレジスタ 1 5 6 には、平文 M の鍵 K_1 が記憶され続けることになる。
- 10

- 図 2 8 は、図 2 0 に示した復号装置に対して鍵 K_1 を保存して再利用する場合の構成を示している。
- 15

図 2 8 は、図 2 0 に対してセクタ 1 7 4 とメモリ 1 7 5 を追加したものである。セクタ 1 7 4 とメモリ 1 7 5 の動作は、図 2 6 に示したセクタ 1 5 4 とメモリ 1 5 5 と同じである。

- メモリ 5 5 とメモリ 1 5 5 は、割り込み I T が発生したときの暗号化装置の状態を記憶するメモリの一例である。このように、メモリ 5 5 とメモリ 1 5 5 とが暗号化処理の状態を記憶しておくことにより、あるデータの暗号化の最中に他のデータの暗号化を行った場合でも、再びあるデータの暗号化の処理に復帰することができる。即ち、メモリ 5 5 に記憶されたデータとメモリ 1 5 5 に記憶された鍵 K とを用いることにより
- 20
- 25 、暗号化が中断されたときと全く同じ状態に暗号化装置を復帰させることができ、中断した暗号化処理を続行させることが可能になる。

なお、メモリ 1 5 5 とメモリ 1 7 5 は、図 6，図 8 に示すメモリ 5 5 と同じ構成のものでもよい。また、図示していないが、図 1 6，図 1 8，図 2 2，図 2 4 に対して、図 2 6，図 2 8 に示すような構成を追加して鍵 K_1 を保存するようにしてもよい。

- 5 また、図 2 6 のメモリ 5 5 とメモリ 1 5 5 とは、同一の動作をするので、1 つのメモリに統合してもよい。また、図 2 8 のメモリ 7 5 とメモリ 1 7 5 とは、同一の動作をするので、1 つのメモリに統合してもよい。

- 10 以上のように、この実施の形態に係る復号装置は、1 つ以上のブロックデータ C_i ($i = 1, 2, 3, \dots, m$) からなる第 1 の処理データ（暗号文 C ）と、1 つ以上のブロックデータ D_j ($j = 1, 2, 3, \dots, n$) からなる第 2 の処理データ（暗号文 D ）との復号処理をする復号装置において、復号処理の状態を記憶するメモリ 7 5 を備え、第 1 の処理データの全ブロックデータ ($C_1 \sim C_m$) の復号処理が完了する前に第 2 の処理データの最初のブロックデータ D_1 の復号処理を開始するとともに、第 2 の処理データの最初のブロックデータ D_1 の復号処理を開始する場合に第 1 の処理データの復号処理の状態を上記メモリに記憶させ、第 1 の処理データの復号処理を再開する場合に復号装置の復号処理の状態をメモリ 7 5 に記憶した第 1 の処理データの復号処理の状態に復帰させてから第 1 の処理データの復号処理を再開することを特徴とする。
- 15
- 20

- 25 また、上記復号装置は、第 2 の処理データの全ブロックデータ ($D_1 \sim D_n$) の復号処理の完了する前に第 1 の処理データの復号処理を再開するとともに、上記メモリ 7 4 は、第 1 の処理データの復号処理を再開する場合に第 2 の処理データの復号処理の状態を記憶し、第 2 の処理データの復号処理を再開する場合は、復号装置の復号処理の状態をメモリ

に記憶した第2の処理データの復号処理の状態に復帰させてから第2の処理データの復号処理を再開することを特徴とする。

ここで、暗号化処理の状態とは、例えば、

図1のCBCモードでは、暗号化ブロックデータ C_i （及び鍵 K_1 ）

5 図16のOFBモードでは、モジュール出力データ T_i （及び鍵 K_1 ）

図18のCFBモードでは、暗号化ブロックデータ C_i （及び鍵 K_1 ）

のことであり、また、復号処理の状態とは、例えば、

10 図20のCBCモードでは、暗号化ブロックデータ C_i （及び鍵 K_1 ）

図22のOFBモードでは、モジュール出力データ T_i （及び鍵 K_1 ）

15 図24のCFBモードでは、暗号化ブロックデータ C_i （及び鍵 K_1 ）

のことである。

前述した説明においては、3つのモードの場合の暗号化装置と復号装置を説明したが、前述した3つのモードは一例であり、これらのモードの改良されたもの、或いは、これらのモードが変形されたものであっても構わない。特に、特徴となる点は、先のブロックデータが暗号化復号されたときに生成されたブロックデータ C_i 又は M_i 又は T_i が次のブロックデータ M_{i+1} 又は C_{i+1} の暗号化復号処理にフィードバックデータとして用いられる暗号化復号方法において、暗号化復号の状態を記憶するメモリ55を設け、他のデータの暗号化復号化の処理後にブロックデータ C_i 又は M_i 又は T_i を用いて再び元の状態に復帰可能にできる点

25 である。従って、特に暗号化モード、復号モードは問わない。

なお、割り込みITを用いず、ポーリング方式やトークン取得方式等の他のメカニズムを用いて暗号化要求を受け付け、2以上の暗号化復号処理のインタラクティブな並列処理を行うようにしてもよい。

また、暗号鍵Kを用いる暗号化復号処理の場合を示したが、暗号鍵K
5 を用いない暗号化復号処理の場合でもよい。

実施の形態2.

この実施の形態においては、暗号化装置が秘匿処理とデータの完全性保証処理を行う場合について説明する。

データの秘匿処理とは、データを暗号化し、データが盗聴されても、
10 或いは、盗まれても意味が分からなくすることである。また、データの完全性保証とは、データが何者かにより置き換えられていることがないことを保証することをいう。データを伝送する場合には、データの秘匿処理を行った上にデータの完全性を保証して伝送したい場合がある。データの秘匿処理は、データを暗号化することにより行われる。データの
15 完全性保証処理は、データの最後に認証子(MAC: Message Authentication Code)を付加し、その認証子を検証することにより改竄を発見することにより行われる。

図29は、OFBモードの暗号化部100により秘匿処理を行い、CBCモードの認証子生成部200により認証子(MAC)を生成する場合を示している。
20

図29は、1つ以上の平文ブロックデータからなる平文を暗号化モジュール51により暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化装置において、平文ブロックデータを暗号化モジュール51により暗号化したときに暗号化モジュール51が
25 出力したモジュール出力ブロックデータ T_i を暗号化モジュール51へ暗号化モジュールへフィードバックする第1のフィードバックループ6

5を有し、平文ブロックデータを入力し、第1のフィードバックループ65によりモジュール出力ブロックデータ T_i をフィードバックさせ暗号化処理を行い、暗号文ブロックデータ C_i を出力する暗号化部100と、認証子演算途中結果 T_i をフィードバックする第2のフィードバックループ66を有し、暗号化部100から暗号文ブロックデータ C_i が出力されるたびに暗号文ブロックデータ C_i を入力し、認証子演算処理を行い、第2のフィードバックループ66により認証子演算途中結果 T_i をフィードバックさせ、暗号文の完全性を保証するための認証子 P を生成する認証子生成部200とを備えたことを特徴とする。

10 図30は、図29に示す暗号化装置の動作手順を示す図である。

平文ブロックデータ M_1 が、まず暗号文ブロックデータ C_1 に暗号化される。次に、平文ブロックデータ M_2 が入力され、暗号文ブロックデータ C_2 に暗号化される。この平文ブロックデータ M_2 の暗号化と同じ時刻に暗号文ブロックデータ C_1 が入力され、認証子の演算が始まる。

15 時刻 T_1 と T_2 の間に平文ブロックデータ M_2 の暗号化と暗号文ブロックデータ C_1 に基づく認証子演算が行われる。また、時刻 T_2 と T_3 の間では、平文ブロックデータ M_3 の暗号化と暗号文ブロックデータ C_2 に基づく認証子の演算が行われる。時刻 T_3 においては、暗号文ブロックデータ C_3 に基づく認証子の演算が行われ、認証子 P が出力される。

20 図29で特徴となる点は、排他的論理和回路58から出力される暗号文ブロックデータ C_i がフィードライン69により排他的論理和回路59に入力されている点である。フィードライン69によりOFBモードとCBCモードの暗号化処理を結合することにより、図30に示すように、秘匿処理と完全性認証処理がパイプライン処理で実行される。図52に示した場合は、時刻 T_6 で処理時間がかかったが、図30の場合は、時刻 T_4 で処理が終了して高速処理が行われたことになる。

図31は、図29に示した暗号化装置の動作フローチャート図である。

5 S51において、ブロックデータカウンタ i を1とする。S52は、暗号化部100の動作であり、暗号化部100は、平文ブロックデータ M_i を入力して平文ブロックデータ M_i を暗号化し、暗号文ブロックデータ C_i を生成して暗号文ブロックデータ C_i を出力する。S53は、認証子生成部200の動作であり、暗号文ブロックデータ C_i を入力し暗号文ブロックデータ C_i を暗号化し、認証子を演算する。S54は、ブロックデータカウンタ i が最後のブロックデータ n を示しているかどうかを判断し、最後のブロックデータでない場合には、S55において、ブロックデータカウンタ i を増加させ、再びS52の処理に戻る。即ち、暗号化部100と認証子生成部200の処理を繰り返す。S54において、最後のブロックデータの処理が終了した場合には、S53で演算された直前の認証子が最終的な認証子であるから、S56において、
10 その認証子を暗号文ブロックデータ C_i の最後に付加する。図31に示すように、暗号化部100が暗号文ブロックデータ C_i を生成するたびに、認証子生成部200が暗号文ブロックデータ C_i を入力して認証子を演算することによりパイプライン処理が可能になり、高速処理が行われる。

20 図32は、図29に示した暗号化部100と認証子生成部200をあわせたものである。即ち、暗号化部100と認証子生成部200の暗号化モジュール51を兼用し、また、暗号化部100と認証子生成部200の排他的論理和回路58と59を兼用したものである。更には、暗号化部100のフィードバックライン65と認証子生成部200のフィードバックライン66を兼用したものである。
25

第1セレクタ61は、秘匿処理の開始時にイニシャルバリュー IV を

選択するものである。第2セレクタ62は、完全性保証処理の開始時に
イニシャルバリューIVを選択するものである。第3セレクタ63は、
秘匿処理と完全性保証処理を交互に選択するものである。第3セレクタ
63は入力をEにすることにより、秘匿処理を行わせることができる。
5 また、第3セレクタ63は入力をFにすることにより、完全性保証処理
を行わせることができる。

メモリ93は、暗号鍵Kを用いた暗号化モジュール51から出力され
たモジュール出力データ T_i を記録するものである。メモリ93は、入
力スイッチ96と出力スイッチ97と第1レジスタ98と第2レジスタ
10 99により構成されている。入力スイッチ96と出力スイッチ97は、
第3セレクタ63の切り替えと同期しており、第3セレクタ63が切り
替わるたびに入力スイッチ96及び出力スイッチ97も切り替わる。

図33は、図32に示す暗号化装置の動作手順を示す図である。

時刻 T_0 と T_1 の間で平文ブロックデータ M_1 の秘匿処理が行われる
15 。秘匿処理の途中で生成されたモジュール出力データは、第1レジスタ
98に記憶される。時刻 T_1 と T_2 の間では、暗号文ブロックデータ C_1
に基づく認証子の演算が行われる。完全性保証処理により生成された
認証子演算途中結果は、第2レジスタ99に記憶される。次に、時刻 T_2
と T_3 の間では、第1レジスタ98に記憶されたモジュール出力デー
20 タと平文ブロックデータ M_2 に基づいて平文ブロックデータ M_2 の秘匿
処理が行われる。次に、時刻 T_3 と T_4 の間では、第2レジスタ99に
記憶された認証子中間演算結果と暗号文ブロックデータ C_2 が入力され
、認証子の演算が行われる。この動作を繰り返すことにより、秘匿処理
と完全性認証処理が完了し、暗号文と認証子Pが出力される。図33に
25 示す場合は、時刻 T_6 までで処理が終了し、時間の短縮は図られてい
ないが、図32に示すように、暗号鍵Kを用いた暗号化モジュール51と

排他的論理和回路 58 とフィードバックライン 67, 68 (フィードバックループ) が兼用されているので、回路規模を小さくすることができる。

図 34 は、OFB モードの復号化部 300 と CBC モードの認証子生成部 400 を有する復号装置を示す図である。

この認証子生成部 400 は、認証子生成部 200 と同一構成のものである。

図 34 は、1 つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子
10 を生成する復号装置において、暗号文ブロックデータ C_i を復号モジュール 71 により復号したときに生成したモジュール出力ブロックデータ T_i をフィードバックする第 1 のフィードバックループ 65 を有し、暗号文ブロックデータ C_i を入力し、第 1 のフィードバックループ 65 によりモジュール出力ブロックデータ T_i をフィードバックさせ復号処理
15 を行い、平文ブロックデータ M_i を出力する復号部 300 と、認証子演算途中結果 T_i をフィードバックする第 2 のフィードバックループ 66 を有し、復号部 300 に入力される暗号文ブロックデータ C_i と同一の暗号文ブロックデータを入力し、認証子演算処理を行い認証子演算途中結果 T_i を出力し、第 2 のフィードバックループ 66 により認証子演算
20 途中結果 T_i をフィードバックさせ、暗号文の完全性を確認するための認証子 Q を生成する認証子生成部 400 とを備えたことを特徴とする。

暗号文ブロックデータ C_i は、復号化部 300 の排他的論理和回路 78 に入力されると同時に、フィードライン 69 により認証子生成部 400 に入力される。このような構成により、復号化部 300 と認証子生成部 400 の処理が同時並列実行され、処理速度が向上する。

図 35 は、図 34 に示した復号装置の復号化部 300 と認証子生成部

400を一体化したものである。

図35は、暗号鍵Kを用いた復号モジュール71とフィードバックライン87、88（フィードバックループ）が兼用されている場合を示している。

- 5 第1セクタ81は、復号処理の開始時にイニシャルバリュースI_Vを選択するものである。第2セクタ82は、完全性保証処理の開始時にイニシャルバリュースI_Vを選択するものである。第3セクタ83は、復号処理と完全性保証処理を交互に選択するものである。第3セクタ83は入力をEにすることにより、復号処理を行わせることができる。
- 10 また、第3セクタ83は入力をFにすることにより、完全性保証処理を行わせることができる。

- メモリ93は、暗号鍵Kを用いた暗号化モジュール51から出力されたモジュール出力データT_iを記録するものである。メモリ93は、入力スイッチ96と出力スイッチ97と第1レジスタ98と第2レジスタ
- 15 99により構成されている。入力スイッチ96と出力スイッチ97は、第3セクタ83の切り替えと同期しており、第3セクタ83が切り替わるたびに入力スイッチ96及び出力スイッチ97も切り替わる。

図36は、図35に示した復号装置の動作手順を示す図である。

復号装置は、暗号文と認証子Pを入力する。

- 20 時刻T₀とT₁の間で暗号文ブロックデータC₁の復号処理と暗号文ブロックデータC₁のレジスタ111への保存が行われる。復号処理の途中で生成されたモジュール出力データは、第1レジスタ98に記憶される。時刻T₁とT₂の間では、レジスタ111に保存された暗号文ブロックデータC₁に基づく認証子の演算が行われる。完全性保証処理により生成された認証子演算途中結果は、第2レジスタ99に記憶される。
- 25 。次に、時刻T₂とT₃の間では、暗号文ブロックデータC₂がレジス

タ 1 1 1 に保存され、第 1 レジスタ 9 8 に記憶されたモジュール出力データと暗号文ブロックデータ C_2 に基づいて平文ブロックデータ M_2 の復号処理が行われる。次に、時刻 T_3 と T_4 の間では、第 2 レジスタ 9 9 に記憶された認証子中間演算結果とレジスタ 1 1 1 に保存された暗号文ブロックデータ C_2 が入力され、認証子の演算が行われる。この動作を繰り返すことにより、平文と認証子 Q が出力される。この認証子 Q は、認証子 P と比較され、認証子 P と認証子 Q が一致していれば、データの完全性が認証できたことになる。これで、復号処理と完全性認証処理が完了する。

10 図 3 7 は、図 2 9 の OFB モードの暗号化部 1 0 0 を CBC モードの暗号化部 1 0 0 にしたものである。

図 3 7 は、1 つ以上の平文ブロックデータからなる平文を暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化装置において、平文ブロックデータを暗号化ユニット 5 2 により暗号化したときに暗号化モジュール 5 1 が出力した暗号文ブロックデータ C_i をフィードバックする第 1 のフィードバックループ 6 5 を有し、平文ブロックデータ M_i を入力し、第 1 のフィードバックループ 6 5 により暗号文ブロックデータ C_i をフィードバックさせ暗号化処理を行い、暗号文ブロックデータ C_i を出力する暗号化部 1 0 0 と、認証子演算途中結果 T_i をフィードバックする第 2 のフィードバックループ 6 6 を有し、暗号化部 1 0 0 から暗号文ブロックデータ C_i が出力されるたびに暗号文ブロックデータ C_i を入力し、認証子演算処理を行い、第 2 のフィードバックループ 6 6 により認証子演算途中結果 T_i をフィードバックさせ、暗号文の完全性を保証するための認証子 P を生成する認証子生成部 4 0 0 とを備えたことを特徴とする。

図 3 8 は、図 3 4 の OFB モードの復号部 3 0 0 を CBC モードの復

号部 300 にしたものである。

図 38 は、1 つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号装置において、暗号文ブロックデータ C_i をフィードバックする第 1 のフィードバックループ 85, 82 を有し、暗号文ブロックデータ C_i を入力し、第 1 のフィードバックループ 85, 82 により暗号文ブロックデータ C_i をフィードバックさせ復号処理を行い、平文ブロックデータ M_i を出力する復号部 300 と、認証子演算途中結果 T_i をフィードバックする第 2 のフィードバックループ 66 を有し、復号部 300 に入力される暗号文ブロックデータ C_i と同一の暗号文ブロックデータ C_i を入力し、認証子演算処理を行い認証子演算途中結果 T_i を出力し、第 2 のフィードバックループにより認証子演算途中結果 T_i をフィードバックさせ、暗号文の完全性を確認するための認証子 Q を生成する認証子生成部 400 とを備えたことを特徴とする。

15 以上のように、図 29, 図 37 は、データを入力して暗号化し、暗号データを出力する暗号化部と、暗号化部が出力した暗号データを入力して暗号文の完全性を保証するための認証子を生成する認証子生成部とを備え、認証子生成部は、暗号化部によるデータの暗号化が完了する前に認証子の生成を開始することを特徴とする暗号化装置を示している。

20 また、図 34, 図 38 は、データを入力して復号し、復号データを出力する復号部と、復号部が入力したデータを入力して暗号文の完全性を保証するための認証子を生成する認証子生成部とを備え、認証子生成部は、復号部によるデータの復号が完了する前に認証子の生成を開始することを特徴とする復号装置を示している。

25 なお、図示していないが、OFB モードの暗号化部 100 又は復号部 300 を用いてもよい。

また、図示していないが、OFBモード又はCFBモードの認証子生成部200を用いてもよい。

図39は、暗号化モジュール51又は復号モジュール71の構成図である。

- 5 暗号化モジュール51は、鍵スケジュール部511とデータランダムライズ部512を有している。鍵スケジュール部511は、1つの鍵Kを入力してn個の拡大鍵 $ExtK_1 \sim ExtK_n$ を生成する。データランダムライズ部512は、関数FとXOR回路とにより乱数を発生させる。関数Fは、拡大鍵を入力して非線形データ変換を行う。
- 10 上記暗号化装置の暗号モジュール51においては、例えば、
- (1) DES (Data Encryption Standard)、又は、
- (2) 国際公開番号WO97/9705 (米国特許出願番号08/83640) に開示されたブロック暗号アルゴリズムであるMISTY、
- 15 又は、
- (3) 上記ブロック暗号アルゴリズムMISTYをベースとした64ビットブロック暗号であり、次世代携帯電話用国際標準暗号 (IMT2000) として採用されることが決定されたブロック暗号アルゴリズムであるKASUMI (詳細は、http://www.3gpp.org/About_3GPP/3gpp.htmを参照のこと)、又は、
- 20 (4) 日本特許出願番号2000-64614 (出願日2000年3月9日) に記載されたブロック暗号アルゴリズムであるCamellia
- a
- などのブロック暗号アルゴリズムを用いることができる。また、上記復
- 25 号装置の復号モジュール71においても、DES、MISTY、KASUMI又はCamelliaなどのブロック暗号アルゴリズムを用いる

ことができる。

図40は、前述した暗号化装置又は復号装置の実装形式を示す図である。

図40は、FPGA又はIC又はLSIの中に前述した暗号化装置及び復号装置が実現されている場合を示している。即ち、前述した暗号化装置及び復号装置は、ハードウェアで実現することができる。また、図示していないが、プリントサーキットボードにより実現することも可能である。

図41は、前述した暗号化装置及び復号装置をソフトウェアで実現する場合を示している。

前述した暗号化装置は、暗号化プログラム47で実現することができる。暗号化プログラム47は、ROM (Read Only Memory) 42 (記録媒体の一例) に記憶されている。暗号化プログラム47は、RAM (Random Access Memory) 又はフレキシブルディスク又は固定ディスク等の他の記録媒体に記録されていてもよい。また、暗号化プログラム47は、サーバコンピュータからダウンロードされてもよい。暗号化プログラム47は、サブルーチンとして機能する。暗号化プログラム47は、RAM 45 に記憶されたアプリケーションプログラム46からサブルーチンコールにより呼び出されて実行される。或いは、暗号化プログラム47は、割り込み制御部43で受け付ける割り込みの発生により起動されるようにしても構わない。メモリ55は、RAM 45の一部であっても構わない。アプリケーションプログラム46、暗号化プログラム47は、CPU 41により実行されるプログラムである。

図42は、アプリケーションプログラム46が暗号化プログラム47を呼び出すメカニズムを示している。

アプリケーションプログラム 46 は、鍵 K とイニシャルバリュー I V と平文 M と暗号文 C をパラメータにして暗号化プログラム 47 を呼び出す。暗号化プログラム 47 は、鍵 K とイニシャルバリュー I V と平文 M を入力し、暗号文 C を返すものである。暗号化プログラム 47 と復号プログラムが同一のときは、鍵 K とイニシャルバリュー I V と暗号文 C と平文 M をパラメータにして暗号化プログラム 47 を呼び出す。

また、図示しないが、暗号化プログラム 47 は、デジタルシグナルプロセッサと、そのデジタルシグナルプロセッサにより読み込まれて実行されるプログラムによって実現しても構わない。即ち、ハードウェアとソフトウェアの組み合わせによって暗号化プログラム 47 を実現しても構わない。

図 40、図 41、図 42 は、主として、暗号化装置の場合を説明したが、復号装置でも同様の方式で実現できる。

図 40 及び図 41 に示したような暗号化装置及び復号装置は、電子機器に対してインストールすることができる。例えば、パーソナルコンピュータやファクシミリ装置や携帯電話やビデオカメラやデジタルカメラやテレビカメラ等のあらゆる電子機器にインストールすることができる。特に、この実施の形態における特徴が発揮できるのは、複数のチャネルからのデータを暗号化復号する場合に有効である。或いは、複数のユーザからのデータがアットランダムに到着して復号する場合に、或いは、複数のユーザに対するデータがアットランダムに発生して、それぞれのデータをリアルタイムに暗号化するような場合に有効である。即ち、暗号化復号するデータの数に比べて暗号化復号する装置の数が少ない場合に、前述した実施の形態の暗号化装置、復号装置が非常に有効である。例えば、多くのクライアントコンピュータをサポートしなければならないサーバコンピュータや多くの携帯電話機からのデータを集配しな

ればならない基地局や回線コントローラなどに、前述した暗号化装置や復号装置が非常に有効である。

なお、暗号化処理同士及び復号処理同士の並列処理でなく、暗号化処理と復号処理との並列処理を行うようにしてもよい。

- 5 また、OFBモードの暗号化部（又は復号化部）とCBCモードの認証子生成部との組み合わせの場合を示したが、OFBモードとCBCモードとCFBモードとこれらのモードの改良モードとその他のモードとのいずれのモードの組み合わせでも構わない。

- 10 また、認証子生成部が、暗号鍵Kを用いた暗号化を行う場合を示したが、認証子生成部は、データの攪拌や演算やその他のデータ処理を行う場合であっても構わない。

産業上の利用可能性

- 15 以上のように、この発明の好適な実施の形態によれば、平文Mの暗号化の途中で平文Nの暗号化を開始することができる。また、暗号文Cの復号中に他の暗号文Dの復号を開始することができる。

また、この発明の好適な実施の形態によれば、優先度を付けることにより暗号化復号されるデータを優先度に基づいて高速に処理することができる。

- 20 また、この発明の好適な実施の形態によれば、秘匿処理と完全性保証処理とを並列処理することにより高速処理が行える。また、秘匿処理と完全性保証処理を統合化された1つのハードウェアで行うことができる。

請求の範囲

1. 第1の処理データと、第2の処理データとの暗号化処理をする暗号化装置において、

5 暗号化処理の状態を記憶するメモリを備え、

第1の処理データの暗号化処理が完了する前に第2の処理データの暗号化処理を開始するとともに、第2の処理データの暗号化処理を開始する場合に第1の処理データの暗号化処理の状態を上記メモリに記憶させ、第1の処理データの暗号化処理を再開する場合に、暗号化装置の暗号化処理の状態を、メモリに記憶した第1の処理データの暗号化処理の状態に復帰させてから第1の処理データの暗号化処理を再開することを特徴とする暗号化装置。

2. 上記暗号化装置は、第2の処理データの暗号化処理の完了する前に第1の処理データの暗号化処理を再開するとともに、上記メモリは、第1の処理データの暗号化処理を再開する場合に第2の処理データの暗号化処理状態を記憶し、第2の処理データの暗号化処理を再開する場合は、暗号化装置の暗号化処理の状態を、メモリに記憶した第2の処理データの暗号化処理の状態に復帰させてから第2の処理データの暗号化処理を再開することを特徴とする請求項1記載の暗号化装置。

20 3. 上記第1の処理データは、第1の平文であり、上記第2の処理データは、第2の平文であることを特徴とする請求項1記載の暗号化装置。

4. 上記暗号化装置は、割り込みにより第2の処理データの暗号化処理を開始することを特徴とする請求項1記載の暗号化装置。

25 5. 平文Mを構成する平文ブロックデータ M_i ($i = 1, 2, 3, \dots$)と平文Nを構成する平文ブロックデータ N_j ($j = 1,$

2, 3, ...) とを暗号化する暗号化装置において、

平文Mの暗号化処理中に平文Nの暗号化要求を平文Mの暗号化処理完了前に受け付けるメカニズムと、

平文ブロックデータ M_i の暗号化処理を行い暗号文ブロックデータ C_i を出力する暗号化ユニットと、

暗号化ユニットから出力された暗号文ブロックデータ C_i をフィードバックラインを介し暗号化ユニットにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記平文Nの暗号化要求を受け付け、平文Nのいずれかの平文ブロックデータの暗号化処理を開始することにより、上記平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化されない場合、フィードバックされる暗号文ブロックデータ C_i を記憶するメモリと、

平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化される場合は、上記フィードバックループのフィードバックラインによりフィードバックされる暗号文ブロックデータ C_i を選択してフィードバックループに供給し、上記平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化されず、平文Nのいずれかの平文ブロックデータの次に暗号化される場合は、上記メモリに記憶された暗号文ブロックデータ C_i を選択してフィードバックループに供給するセレクトと

を備えたことを特徴とする暗号化装置。

6. 上記メモリは、

複数の平文に対応した複数のレジスタと、

暗号化処理をする平文に対応してレジスタを切り替えるスイッチとを備えたことを特徴とする請求項5記載の暗号化装置。

7. 暗号化モジュールから出力される暗号文ブロックデータ C_i ($i = 1, 2, 3, \dots$) を用いて第1の平文Mの平文ブロックデータ M_i ($i = 1, 2, 3, \dots$) を暗号化する工程と、

5 上記平文ブロックデータ M_i を暗号化している途中で又は平文ブロックデータ M_i を暗号化した後に、第1の平文Mの平文ブロックデータ M_{i+1} の暗号化に用いられる暗号文ブロックデータ C_i をメモリに記憶する工程と、

10 上記平文ブロックデータ M_{i+1} の暗号化に用いられる暗号文ブロックデータ C_i をメモリに記憶した後に、第2の平文Nの少なくとも1つの平文ブロックデータを暗号化する工程と、

15 上記第2の平文Nの少なくとも1つの平文ブロックデータを暗号化した後に、メモリに記憶された、平文ブロックデータ M_{i+1} の暗号化に用いられる暗号文ブロックデータ C_i を入力し、暗号化モジュールを用いて第1の平文Mの平文ブロックデータ M_{i+1} を暗号化する工程とを備えたことを特徴とする暗号化方法。

8. 1つ以上の平文ブロックデータからなる平文を暗号化ユニット暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化装置において、

20 平文ブロックデータを暗号化ユニットにより暗号化したときに暗号化ユニットが出力した暗号文ブロックデータ C_i を暗号化ユニットへフィードバックする第1のフィードバックループを有し、平文ブロックデータを入力し、第1のフィードバックループにより暗号文ブロックデータ C_i をフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化部と、

25 認証子演算途中結果をフィードバックする第2のフィードバックループを有し、暗号化部から暗号文ブロックデータが出力されるたびに暗号

文ブロックデータを入力し、データ処理を行い、第2のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成部とを備えたことを特徴とする暗号化装置。

- 5 9. 上記暗号化部と認証子生成部とは、1つの暗号化モジュールと、1つのフィードバックループとを兼用して暗号化処理と認証子生成処理とを交互に行うとともに、

上記1つのフィードバックループは、

- 暗号化処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、
10

暗号化処理と認証生成処理とを交互に実行するために、メモリから暗号化処理と認証子生成処理との結果を交互に選択して暗号化モジュールに出力するセレクタと

を備えたことを特徴とする請求項8記載の暗号化装置。

- 15 10. 1つ以上の平文ブロックデータからなる平文を暗号化ユニットにより暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化方法において、

- 平文ブロックデータを暗号化ユニットにより暗号化したときに暗号化ユニットが出力した暗号文ブロックデータ C_i を暗号化ユニットへフィードバックする第1のフィードバック工程を有し、平文ブロックデータ
20 を入力し、第1のフィードバックループにより暗号文ブロックデータ C_i をフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化工程と、

- 認証子演算途中結果をフィードバックする第2のフィードバック工程
25 を有し、暗号化工程から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第2のフィードバック

工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成工程とを備えたことを特徴とする暗号化方法。

5 1 1. 第 1 の処理データと、第 2 の処理データとの復号処理をする復号装置において、

復号処理の状態を記憶するメモリを備え、

10 第 1 の処理データの復号処理が完了する前に第 2 の処理データの復号処理を開始するとともに、第 2 の処理データの復号処理を開始する場合に第 1 の処理データの復号処理の状態を上記メモリに記憶させ、第 1 の処理データの復号処理を再開する場合に、復号装置の復号処理の状態を、メモリに記憶した第 1 の処理データの復号処理の状態に復帰させてから第 1 の処理データの復号処理を再開することを特徴とする復号装置。

15 1 2. 上記復号装置は、第 2 の処理データの復号処理の完了する前に第 1 の処理データの復号処理を再開するとともに、上記メモリは、第 1 の処理データの復号処理を再開する場合に第 2 の処理データの復号処理状態を記憶し、第 2 の処理データの復号処理を再開する場合は、復号装置の復号処理の状態を、メモリに記憶した第 2 の処理データの復号処理の状態に復帰させてから第 2 の処理データの復号処理を再開することを特徴とする請求項 1 1 記載の復号装置。

20 1 3. 上記第 1 の処理データは、第 1 の暗号文であり、上記第 2 の処理データは、第 2 の暗号文であることを特徴とする請求項 1 1 記載の復号装置。

25 1 4. 上記復号装置は、割り込みにより第 2 の処理データの最初のブロックデータの復号処理を開始することを特徴とする請求項 1 1 記載の復号装置。

1 5. 暗号文 C を構成する暗号文ブロックデータ C_i ($i = 1$

、 2、 3、 …）と暗号文Dを構成する暗号文ブロックデータ D_j （ $j = 1, 2, 3, \dots$ ）とを復号する復号装置において、

暗号文Cの復号処理中に暗号文Dの復号要求を任意の時点で受け付けるメカニズムと、

- 5 暗号文ブロックデータ C_i の復号処理を行い平文ブロックデータ M_i を出力する復号ユニットと、

暗号文ブロックデータ C_{i+1} を復号するための暗号文ブロックデータ C_i をフィードバックラインを介し復号ユニットにフィードバックするフィードバックループと、

- 10 フィードバックループのフィードバックラインと並列に設けられ、上記暗号文Dの復号要求を受け付け、暗号文Dのいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号されない場合、フィードバックされる暗号文ブロックデータ C_i を記憶するメモリと、

- 15 暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号される場合は、上記フィードバックループのフィードバックラインによりフィードバックされる暗号文ブロックデータ C_i を選択してフィードバックループに供給し、上記暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号されず、暗号文Dのいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリに記憶された暗号文ブロックデータ C_i を選択してフィードバックループに供給するセレクトと

を備えたことを特徴とする復号装置。

16. 上記メモリは、

- 25 複数の暗号文に対応した複数のレジスタと、
復号処理をする暗号文に対応してレジスタを切り替えるスイッチと

を備えたことを特徴とする請求項 1 5 記載の復号装置。

1 7. 復号モジュールを用いて第 1 の暗号文 C の暗号文ブロックデータ C_i ($i = 1, 2, 3, \dots$) を復号する工程と、

5 上記暗号文ブロックデータ C_i を復号している途中で又は暗号文ブロックデータ C_i を復号した後に、第 1 の暗号文 C の暗号文ブロックデータ C_{i+1} の復号に用いられる暗号文ブロックデータ C_i をメモリに記憶する工程と、

10 上記暗号文ブロックデータ C_{i+1} の復号に用いられる暗号文ブロックデータ C_i をメモリに記憶した後に、第 2 の暗号文 D の少なくとも 1 つの暗号文ブロックデータを復号する工程と、

15 上記第 2 の暗号文 D の少なくとも 1 つの暗号文ブロックデータを復号した後に、メモリに記憶された、暗号文ブロックデータ C_{i+1} の復号に用いられる暗号文ブロックデータ C_i を入力し、復号モジュールを用いて第 1 の暗号文 C の暗号文ブロックデータ C_{i+1} を復号する工程とを備えたことを特徴とする復号方法。

1 8. 1 つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号装置において、

20 復号モジュールによりデータを復号したときに生成したモジュール出力ブロックデータ T_i を復号モジュールへフィードバックする第 1 のフィードバックループを有し、暗号文ブロックデータを入力し、第 1 のフィードバックループによりモジュール出力ブロックデータ T_i をフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号部と、

25 認証子演算途中結果をフィードバックする第 2 のフィードバックループを有し、復号部に入力される暗号文ブロックデータと同一の暗号文ブ

ロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第2のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成部と

5 を備えたことを特徴とする復号装置。

19. 上記復号部と認証子生成部とは、1つの復号モジュールと、1つのフィードバックループとを兼用して復号処理と認証子生成処理とを交互に行うとともに、

上記1つのフィードバックループは、

10 復号処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

復号処理と認証子生成処理とを交互に実行するために、メモリから復号処理と認証子生成処理との結果を交互に選択して復号モジュールに出力するセレクタと

15 を備えたことを特徴とする請求項18記載の復号装置。

20. 1つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号方法において、

20 復号モジュールによりデータを復号したときに生成したモジュール出力ブロックデータ T_i を復号モジュールへフィードバックする第1のフィードバック工程を有し、暗号文ブロックデータを入力し、第1のフィードバックループによりモジュール出力ブロックデータ T_i をフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号工程と、

25 認証子演算途中結果をフィードバックする第2のフィードバック工程を有し、復号工程に入力される暗号文ブロックデータと同一の暗号文ブ

ロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第2のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成工程と

5 を備えたことを特徴とする復号方法。

2 1. 平文Mを構成する平文ブロックデータ M_i ($i = 1, 2, 3, \dots$)と平文Nを構成する平文ブロックデータ N_j ($j = 1, 2, 3, \dots$)とを暗号化する暗号化装置において、

10 平文Mの暗号化処理中に平文Nの暗号化要求を平文Mの暗号化処理完了前に受け付けるメカニズムと、

暗号化処理を行ったデータをモジュール出力ブロックデータ T_i として出力する暗号化モジュールと、

15 暗号化モジュールから出力されたモジュール出力ブロックデータ T_i をフィードバックラインを介し暗号化モジュールにフィードバックするフィードバックループと、

20 フィードバックループのフィードバックラインと並列に設けられ、上記平文Nの暗号化要求を受け付け、平文Nのいずれかの平文ブロックデータの暗号化処理を開始することにより、上記平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化されない場合、フィードバックされるモジュール出力ブロックデータ T_i を記憶するメモリと、

25 平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化される場合は、上記フィードバックループのフィードバックラインによりフィードバックされるモジュール出力ブロックデータ T_i を選択してフィードバックループに供給し、上記平文ブロックデータ M_{i+1} が平文ブロックデータ M_i の次に続けて暗号化されず、平文Nのいずれか

の平文ブロックデータの次に暗号化される場合は、上記メモリに記憶されたモジュール出力ブロックデータ T_i を選択してフィードバックループに供給するセクタと
を備えたことを特徴とする暗号化装置。

5 2 2. 上記メモリは、

複数の平文に対応した複数のレジスタと、
暗号化処理をする平文に対応してレジスタを切り替えるスイッチと
を備えたことを特徴とする請求項 2 1 記載の暗号化装置。

2 3. 暗号化モジュールから出力されるモジュール出力ブロッ
10 クデータ T_i ($i = 1, 2, 3, \dots$) を用いて第 1 の平文 M の平文
ブロックデータ M_i ($i = 1, 2, 3, \dots$) を暗号化する工程と、

上記平文ブロックデータ M_i を暗号化している途中で又は平文ブロッ
クデータ M_i を暗号化した後に、第 1 の平文 M の平文ブロックデータ M_{i+1}
15 の暗号化に用いられるモジュール出力ブロックデータ T_i をメモリ
に記憶する工程と、

上記平文ブロックデータ M_{i+1} の暗号化に用いられるモジュール出力
ブロックデータ T_i をメモリに記憶した後に、第 2 の平文 N の少なくとも
も 1 つの平文ブロックデータを暗号化する工程と、

上記第 2 の平文 N の少なくとも 1 つの平文ブロックデータを暗号化し
20 た後に、メモリに記憶された、平文ブロックデータ M_{i+1} の暗号化に用
いられるモジュール出力ブロックデータ T_i を入力し、暗号化モジュール
を用いて第 1 の平文 M の平文ブロックデータ M_{i+1} を暗号化する工程
と

を備えたことを特徴とする暗号化方法。

25 2 4. 1 つ以上の平文ブロックデータからなる平文を暗号化モ
ジュールにより暗号文にし、暗号文に対して暗号文の完全性を保証する

ための認証子を生成する暗号化装置において、

平文ブロックデータを暗号化モジュールにより暗号化したときに暗号化モジュールが出力したモジュール出力ブロックデータ T_i を暗号化モジュールへフィードバックする第1のフィードバックループを有し、平文ブロックデータを入力し、第1のフィードバックループによりモジュール出力ブロックデータ T_i をフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化部と、

認証子演算途中結果をフィードバックする第2のフィードバックループを有し、暗号化部から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第2のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成部とを備えたことを特徴とする暗号化装置。

25. 上記暗号化部と認証子生成部とは、1つの暗号化モジュールと、1つのフィードバックループとを兼用して暗号化処理と認証子生成処理とを交互に行うとともに、

上記1つのフィードバックループは、

暗号化処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

暗号化処理と認証生成処理とを交互に実行するために、メモリから暗号化処理と認証子生成処理との結果を交互に選択して暗号化モジュールに出力するセレクタと

を備えたことを特徴とする請求項24記載の暗号化装置。

26. 1つ以上の平文ブロックデータからなる平文を暗号化モジュールにより暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化方法において、

平文ブロックデータを暗号化モジュールにより暗号化したときに暗号化モジュールが出力したモジュール出力ブロックデータ T_i を暗号化モジュールへフィードバックする第1のフィードバック工程を有し、平文ブロックデータを入力し、第1のフィードバックループによりモジュール出力ブロックデータ T_i をフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化工程と、

認証子演算途中結果をフィードバックする第2のフィードバック工程を有し、暗号化工程から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第2のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成工程とを備えたことを特徴とする暗号化方法。

27. 暗号文Cを構成する暗号文ブロックデータ C_i ($i = 1, 2, 3, \dots$) と暗号文Dを構成する暗号文ブロックデータ D_j ($j = 1, 2, 3, \dots$) とを復号する復号装置において、

暗号文Cの復号処理中に暗号文Dの復号要求を任意の時点で受け付けるメカニズムと、

復号処理を行ったデータをモジュール出力ブロックデータ T_i として出力する復号モジュールと、

復号モジュールから出力されたモジュール出力ブロックデータ T_i をフィードバックラインを介し復号モジュールにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記暗号文Dの復号要求を受け付け、暗号文Dのいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号されない場合、フ

ィードバックされるモジュール出力ブロックデータ T_i を記憶するメモリと、

- 5 暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号される場合は、上記フィードバックループのフィードバックラインによりフィードバックされるモジュール出力ブロックデータ T_i を選択してフィードバックループに供給し、上記暗号文ブロックデータ C_{i+1} が暗号文ブロックデータ C_i の次に続けて復号されず、暗号文Dのいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリに記憶されたモジュール出力ブロックデータ T_i を選択してフィードバック
- 10 クループに供給するセクタと
- を備えたことを特徴とする復号装置。

28. 上記メモリは、

複数の暗号文に対応した複数のレジスタと、

- 復号処理をする暗号文に対応してレジスタを切り替えるスイッチと
- 15 を備えたことを特徴とする請求項27記載の復号装置。

29. 復号モジュールから出力されるモジュール出力ブロックデータ T_i ($i = 1, 2, 3, \dots$) を用いて第1の暗号文Cの暗号文ブロックデータ C_i ($i = 1, 2, 3, \dots$) を復号する工程と、

- 上記暗号文ブロックデータ C_i を復号している途中で又は暗号文ブロックデータ C_i を復号した後に、第1の暗号文Cの暗号文ブロックデータ C_{i+1} の復号に用いられるモジュール出力ブロックデータ T_i をメモリに記憶する工程と、
- 20

- 上記暗号文ブロックデータ C_{i+1} の復号に用いられるモジュール出力ブロックデータ T_i をメモリに記憶した後に、第2の暗号文Dの少なくとも1つの暗号文ブロックデータを復号する工程と、
- 25

上記第2の暗号文Dの少なくとも1つの暗号文ブロックデータを復号

した後に、メモリに記憶された、暗号文ブロックデータ C_{i+1} の復号に用いられるモジュール出力ブロックデータ T_i を入力し、復号モジュールを用いて第 1 の暗号文 C の暗号文ブロックデータ C_{i+1} を復号する工程と

5 を備えたことを特徴とする復号方法。

30. 1つ以上の暗号文ブロックデータからなる暗号文を復号ユニットにより平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号装置において、

10 暗号文ブロックデータ C_i を復号ユニットへフィードバックする第 1 のフィードバックループを有し、暗号文ブロックデータを入力し、第 1 のフィードバックループにより暗号文ブロックデータ C_i をフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号部と、

15 認証子演算途中結果をフィードバックする第 2 のフィードバックループを有し、復号部に入力される暗号文ブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第 2 のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成部と

を備えたことを特徴とする復号装置。

20 31. 上記復号部と認証子生成部とは、1つの復号モジュールと、1つのフィードバックループとを兼用して復号処理と認証子生成処理とを交互に行うとともに、

上記 1 つのフィードバックループは、

25 復号処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

復号処理と認証生成処理とを交互に実行するために、メモリから復号

処理と認証子生成処理との結果を交互に選択して復号モジュールに出力するセレクトと

を備えたことを特徴とする請求項 30 記載の復号装置。

32. 1つ以上の暗号文ブロックデータからなる暗号文を復号
5 ユニットにより平文に復号し、かつ、暗号文に対して暗号文の完全性を
確認するための認証子を生成する復号方法において、

暗号文ブロックデータ C_i を復号ユニットへフィードバックする第1
のフィードバック工程を有し、暗号文ブロックデータを入力し、第1の
フィードバックループにより暗号文ブロックデータ C_i をフィードバッ
10 クさせ復号処理を行い、平文ブロックデータを出力する復号工程と、

認証子演算途中結果をフィードバックする第2のフィードバック工程
を有し、復号工程に入力される暗号文ブロックデータと同一の暗号文ブ
ロックデータを入力し、データ処理を行い認証子演算途中結果を出力し
、第2のフィードバック工程により認証子演算途中結果をフィードバッ
15 クさせ、暗号文の完全性を確認するための認証子を生成する認証子生成
工程と

を備えたことを特徴とする復号方法。

33. 上記請求項7記載の暗号化方法の各工程をコンピュータ
に実行させるためのプログラムを記録したコンピュータ読み取り可能な
20 記録媒体。

34. 上記請求項10記載の暗号化方法の各工程をコンピュータ
に実行させるためのプログラムを記録したコンピュータ読み取り可能
な記録媒体。

35. 上記請求項17記載の復号方法の各工程をコンピュータ
25 に実行させるためのプログラムを記録したコンピュータ読み取り可能な
記録媒体。

36. 上記請求項20記載の復号方法の各工程をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

5 37. 上記請求項23記載の暗号化方法の各工程をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

38. 上記請求項26記載の暗号化方法の各工程をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

10 39. 上記請求項29記載の復号方法の各工程をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

15 40. 上記請求項32記載の復号方法の各工程をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

41. 上記暗号化処理は、ブロック暗号アルゴリズムを用いることを特徴とする請求項1記載の暗号化装置。

42. 上記復号処理は、ブロック暗号アルゴリズムを用いることを特徴とする請求項11記載の復号装置。

20 43. 上記メモリは、暗号化処理の状態として、
第1の処理データの暗号化途中結果と、
第1の処理データを暗号化するために用いる暗号鍵と
を記憶することを特徴とする請求項1記載の暗号化装置。

25 44. 上記メモリは、復号処理の状態として、
第2の処理データの復号途中結果と、
第2の処理データを復号するために用いる復号鍵と

を記憶することを特徴とする請求項 1 1 記載の復号装置。

4 5. データを入力して暗号化し、暗号データを出力する暗号化部と、

5 暗号化部が出力した暗号データを入力して暗号文の完全性を保証するための認証子を生成する認証子生成部とを備え、

認証子生成部は、暗号化部によるデータの暗号化が完了する前に認証子の生成を開始することを特徴とする暗号化装置。

10 4 6. データを入力して復号し、復号データを出力する復号部と、

復号部が入力したデータを入力して暗号文の完全性を保証するための認証子を生成する認証子生成部とを備え、

15 認証子生成部は、復号部によるデータの復号が完了する前に認証子の生成を開始することを特徴とする復号装置。

4 7. データを入力して暗号化し、暗号データを出力する暗号化工程と、

20 暗号化工程が出力した暗号データを入力して暗号文の完全性を保証するための認証子を生成する認証子生成工程とを備え、

認証子生成工程は、暗号化工程によるデータの暗号化が完了する前に認証子の生成を開始することを特徴とする暗号化方法。

4 8. データを入力して復号し、復号データを出力する復号工程と、

25 復号工程が入力したデータを入力して暗号文の完全性を保証するための認証子を生成する認証子生成工程と

を備え、

認証子生成工程は、復号工程によるデータの復号が完了する前に認証子の生成を開始することを特徴とする復号方法。

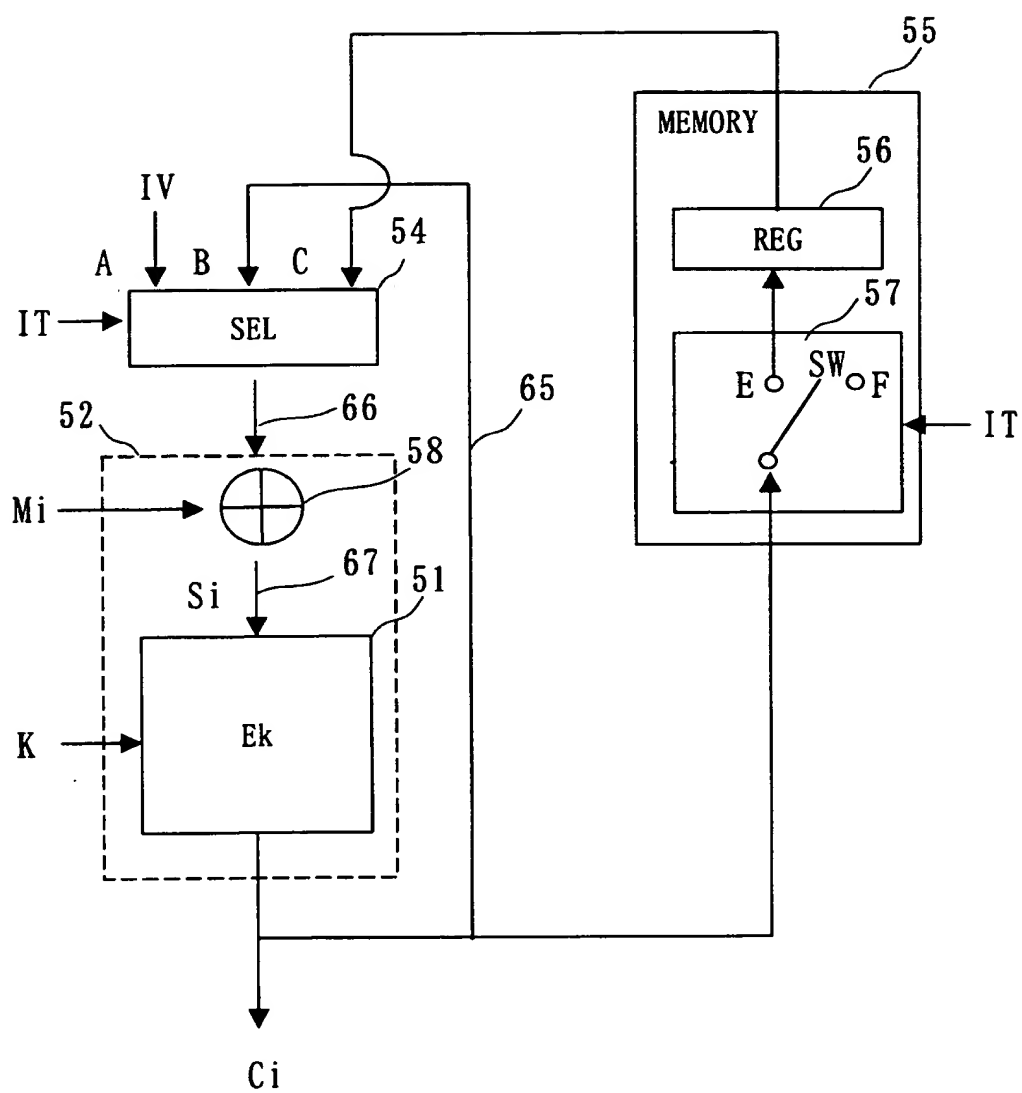
49. 上記請求項47記載の暗号化方法の各工程をコンピュータ
5 に実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

50. 上記請求項48記載の復号方法の各工程をコンピュータ
に実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

This Page Blank (uspto)

1/49

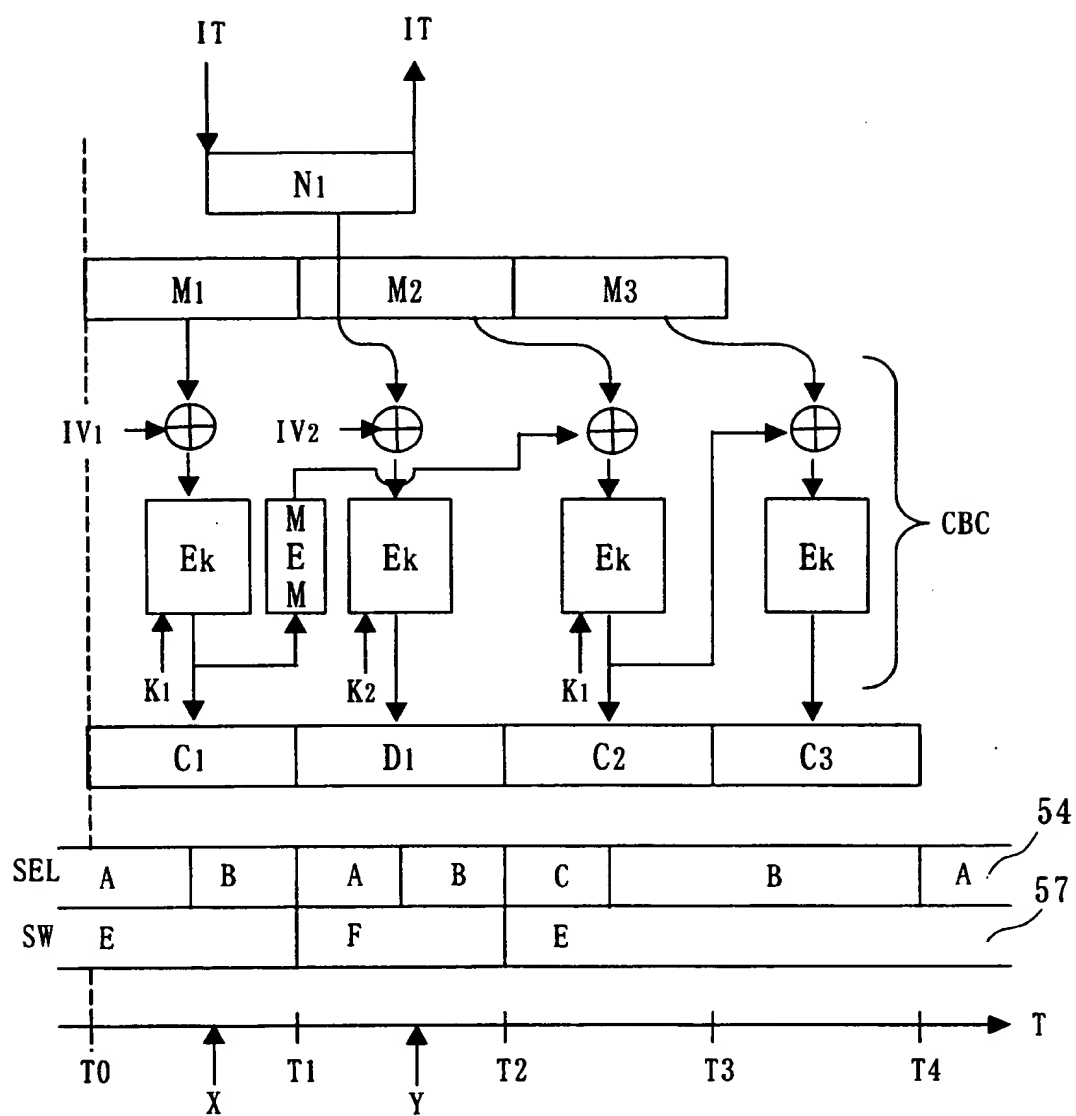
図 1



This Page Blank (uspto)

2/49

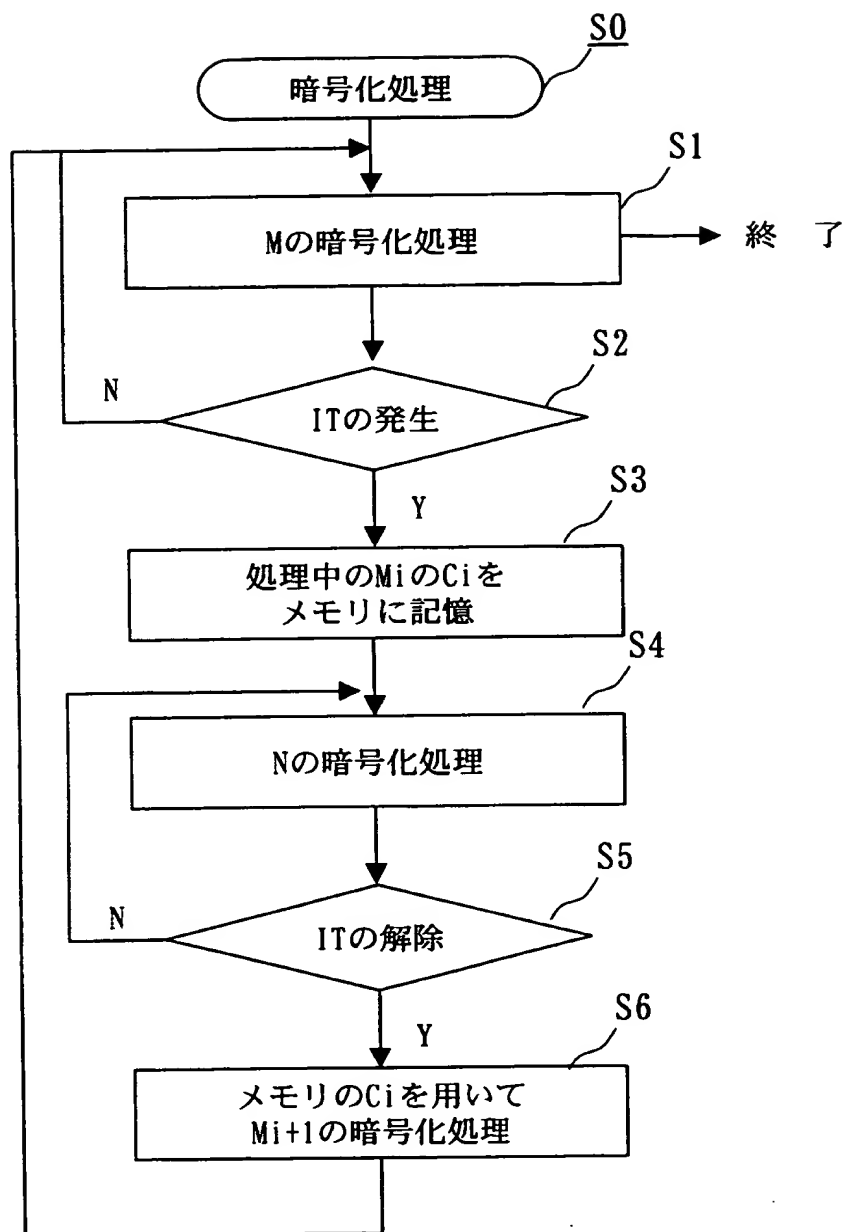
図 2



This Page Blank (uspto)

3/49

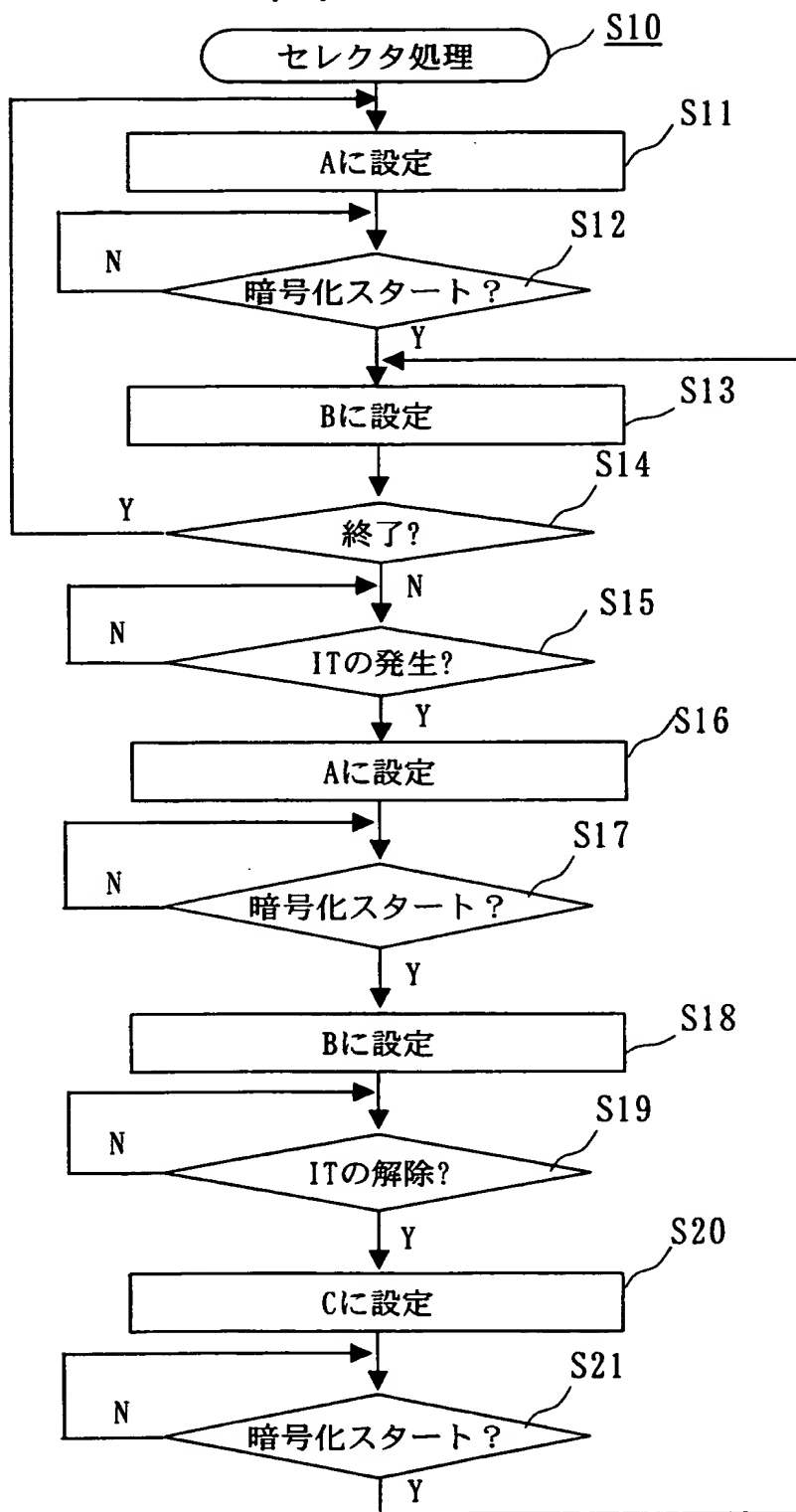
図 3



This Page Blank (uspto)

4/49

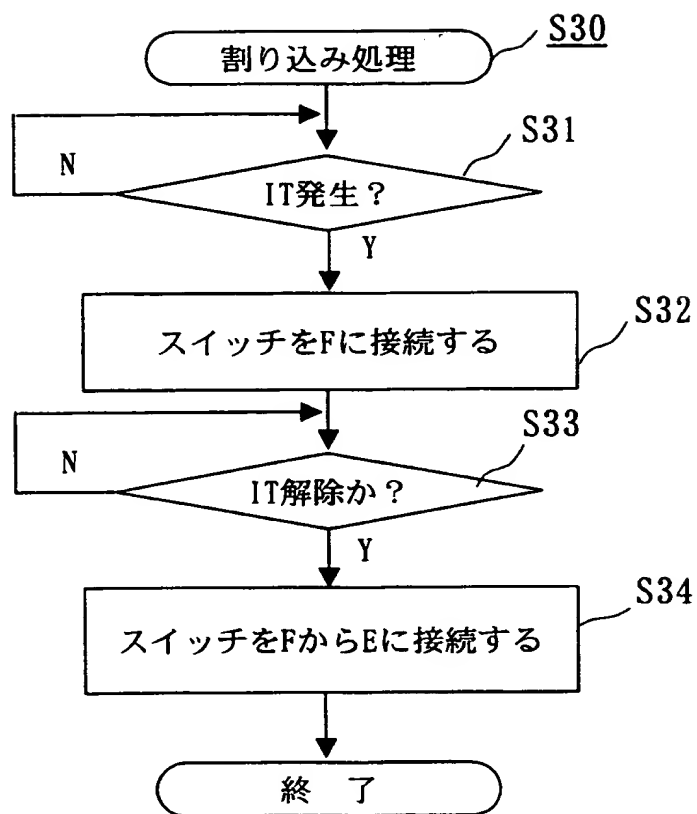
図 4



This Page Blank (uspto)

5/49

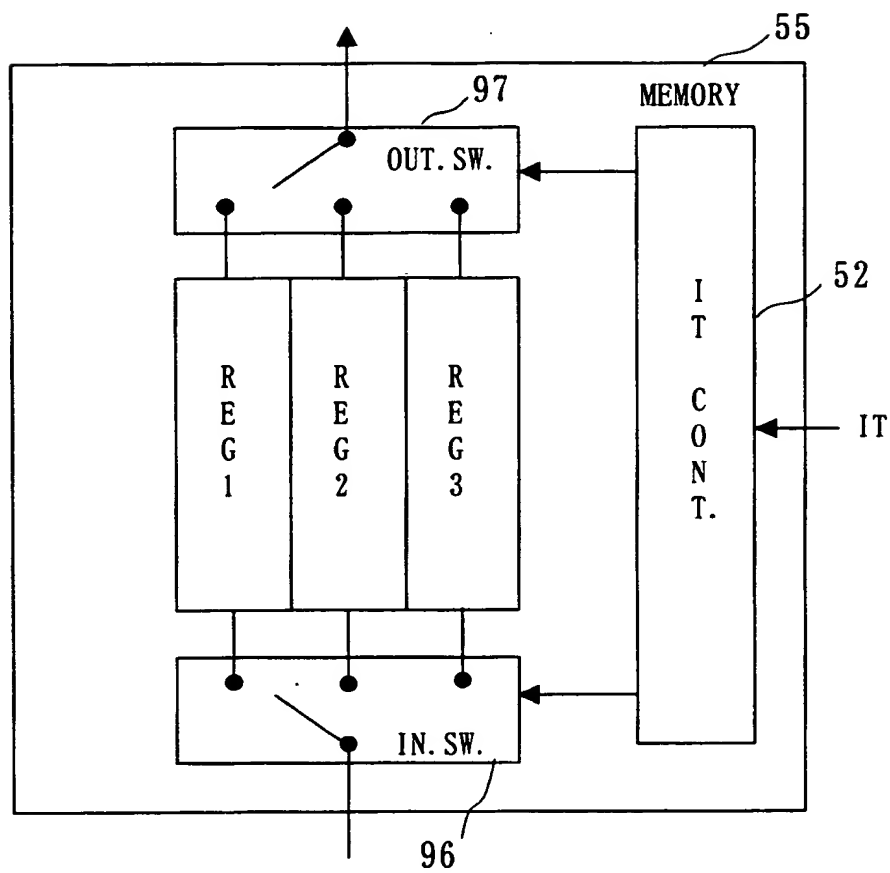
図 5



This Page Blank (uspto)

6/49

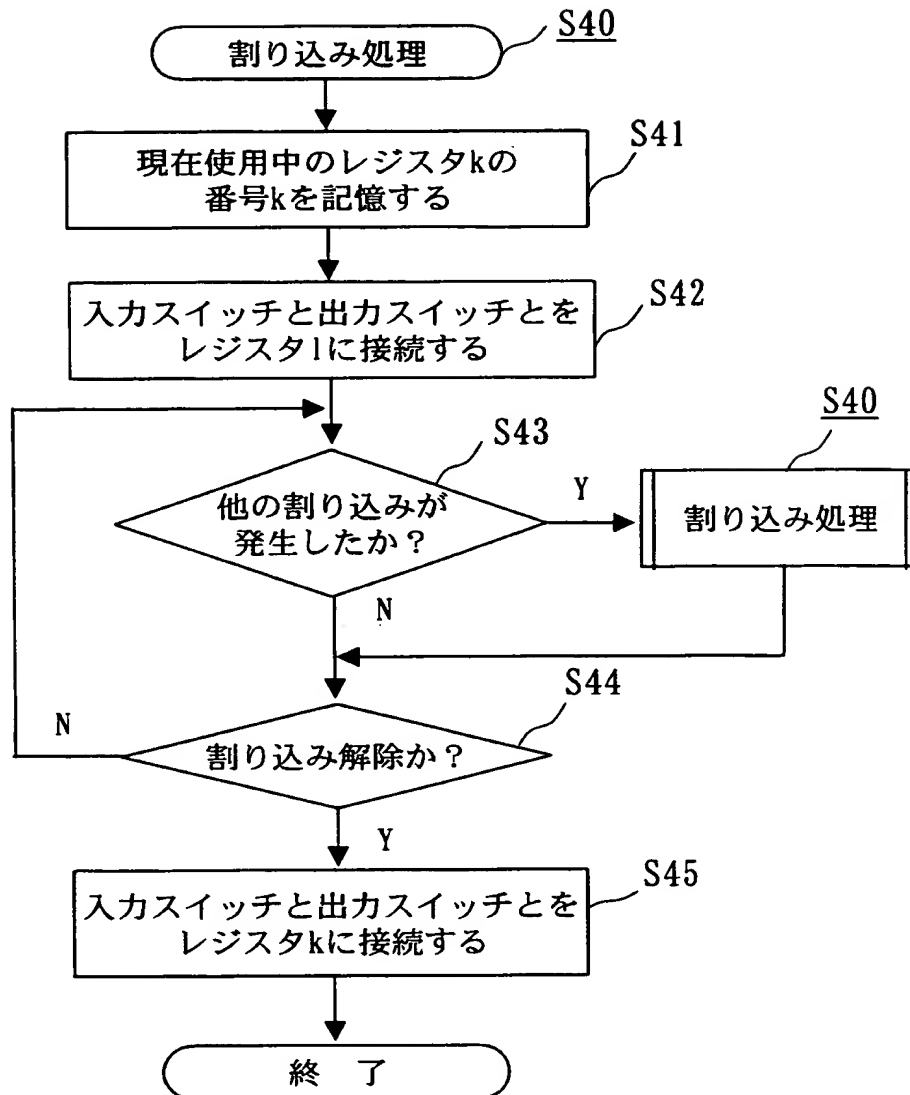
図 6



This Page Blank (uspto)

7/49

図 7



This Page Blank (uspto)

8/49

図 8

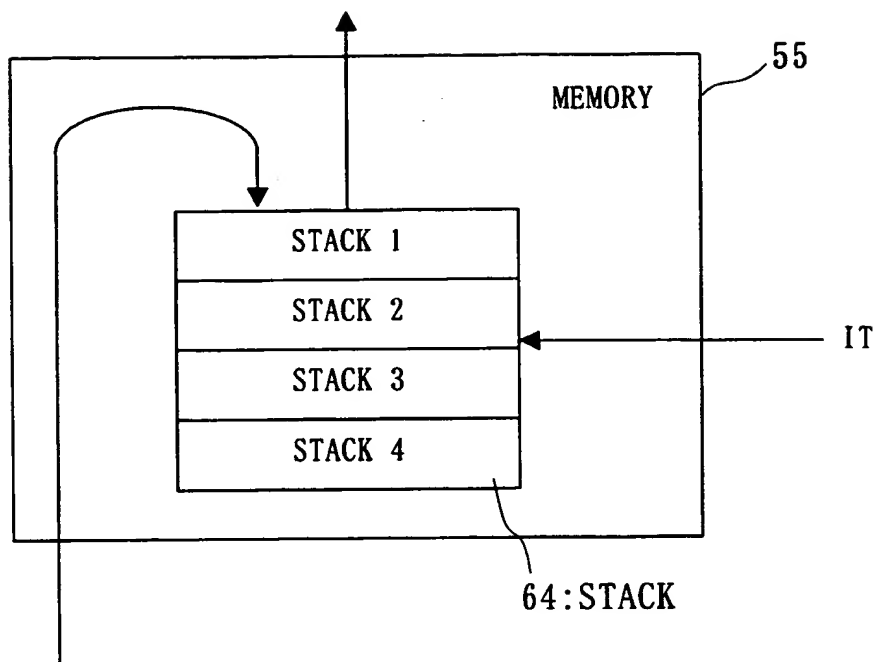
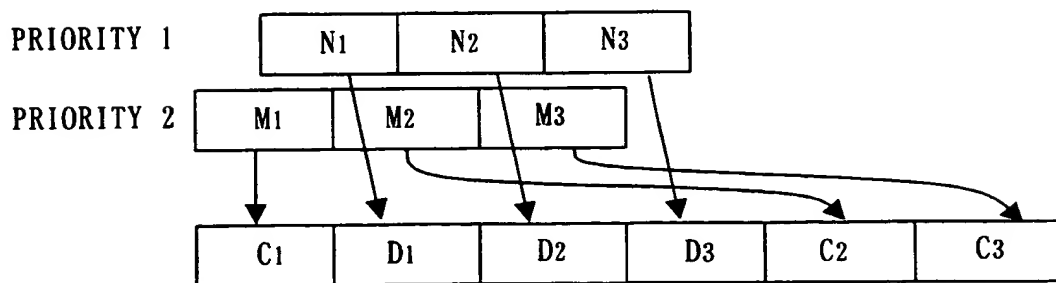


図 9



This Page Blank (uspto)

9/49

図10

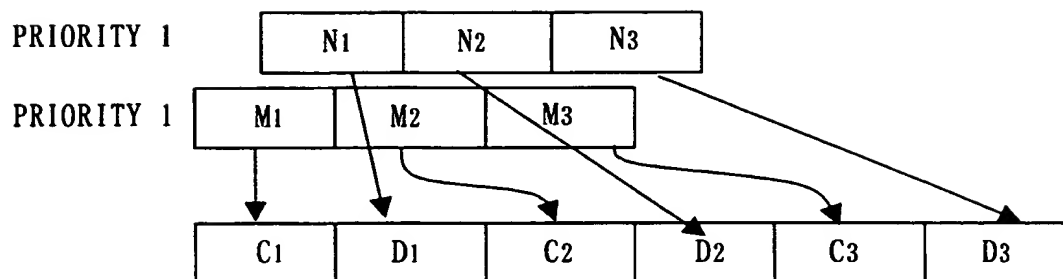
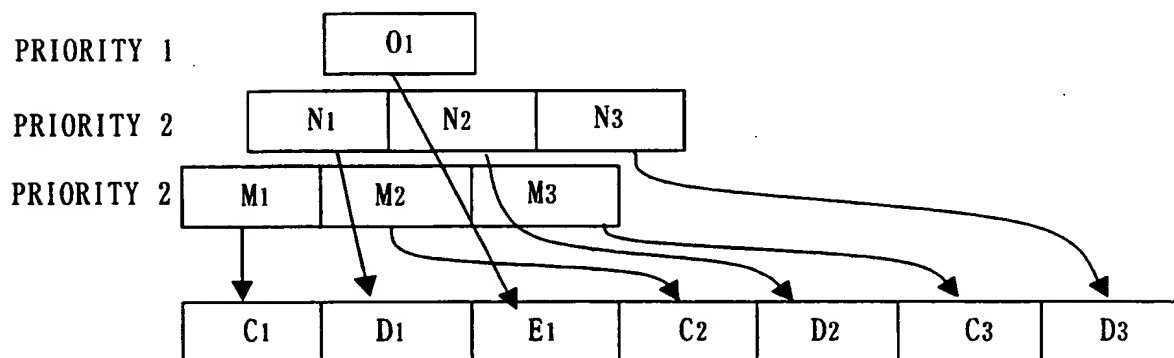


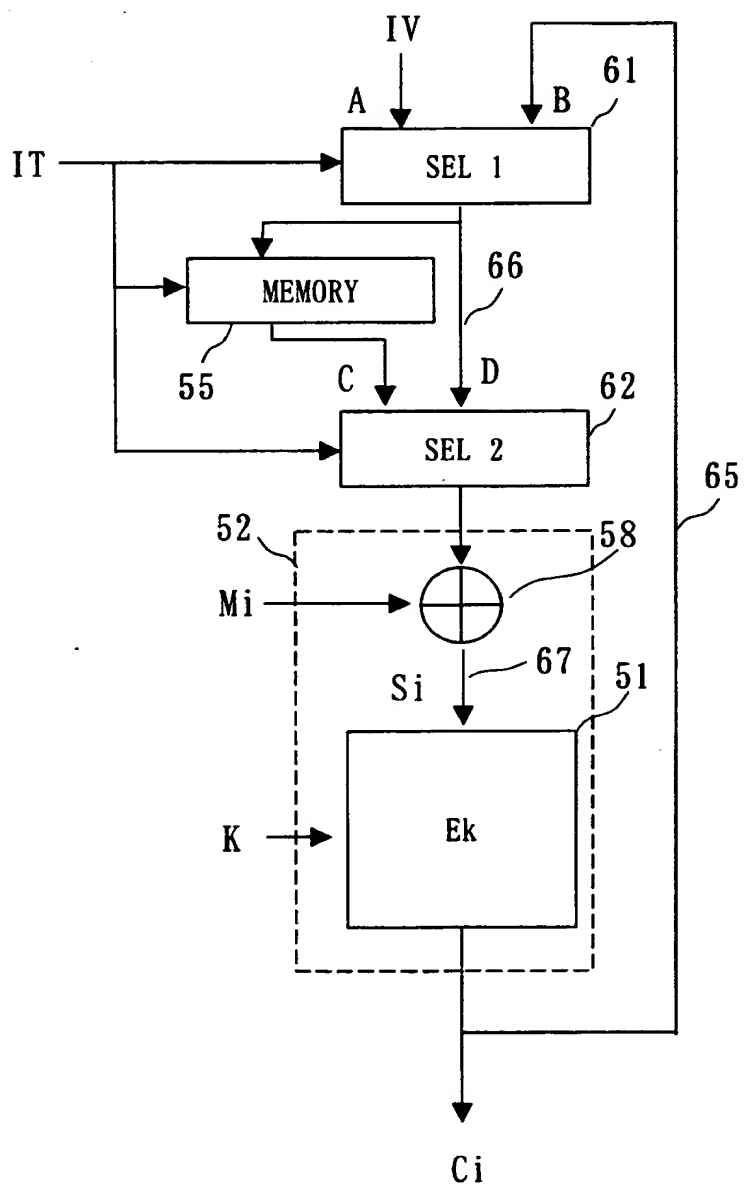
図11



This Page Blank (uspto)

10/49

図12

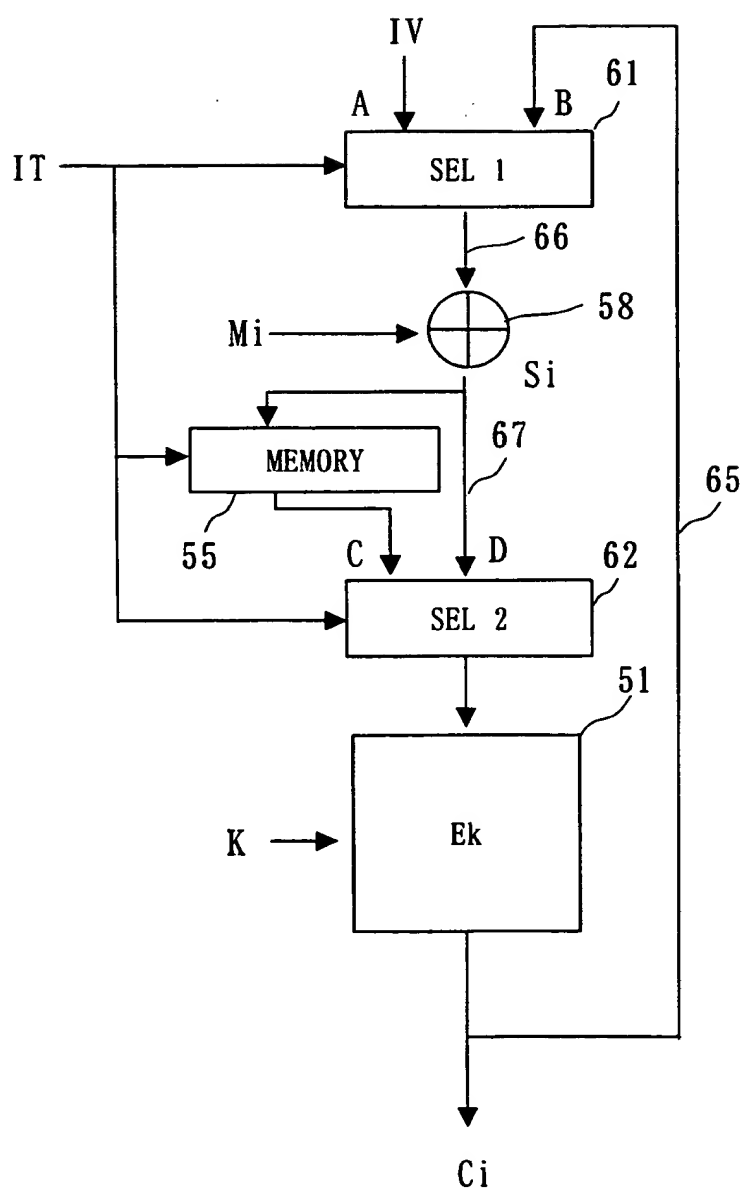


This Page Blank (uspto)

This Page Blank (uspto)

12/49

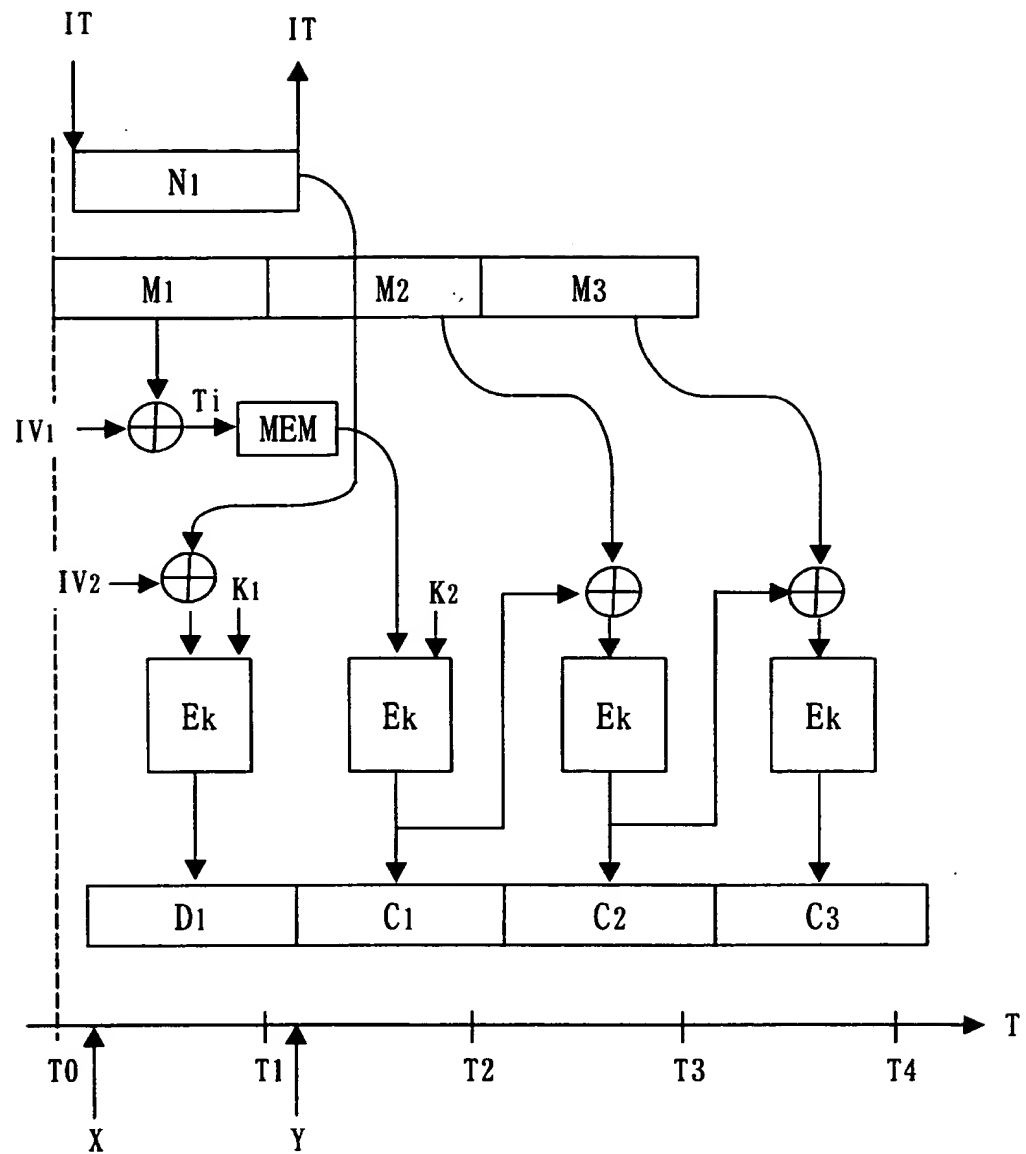
図14



Inis Page Blank (uspto)

13 / 49

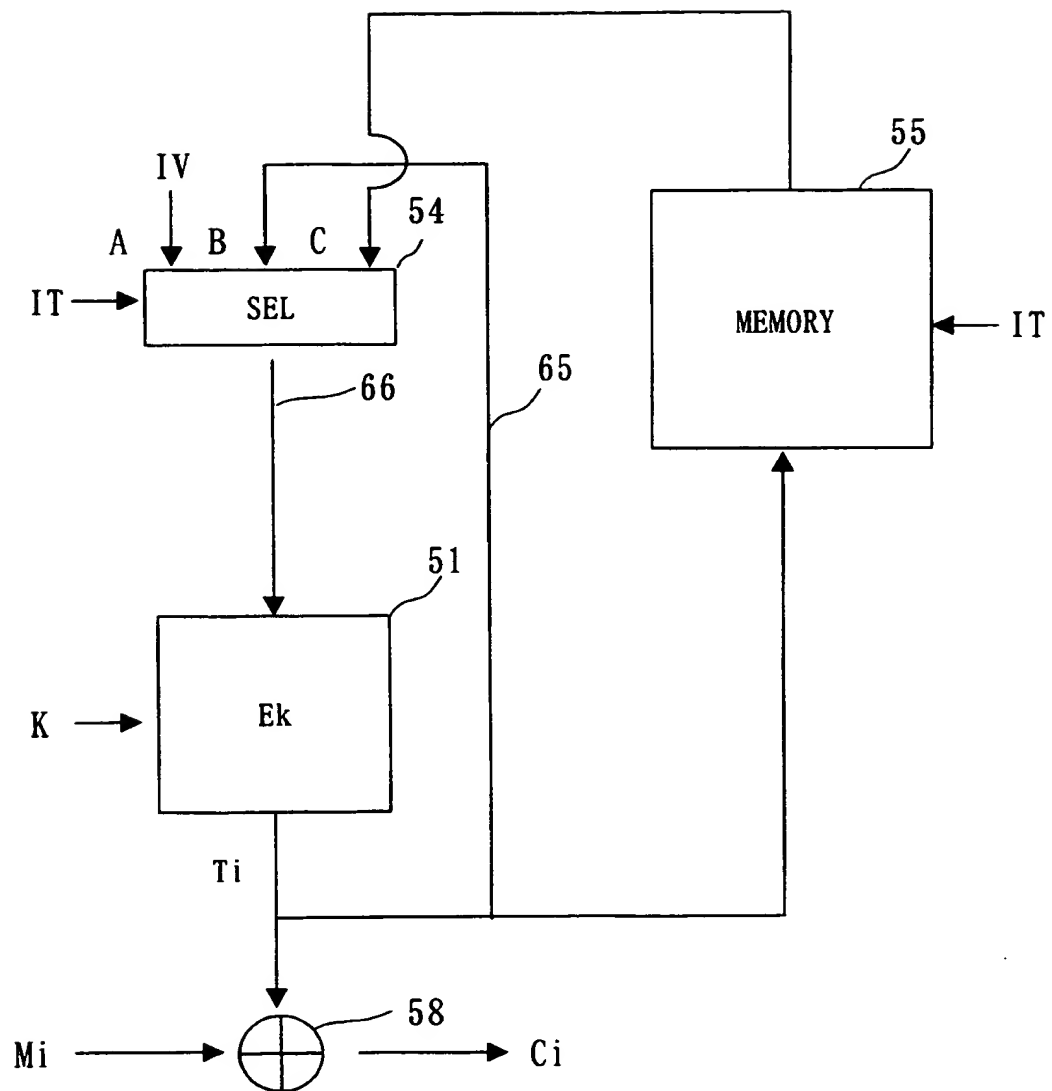
図 15



This Page Blank (uspto)

14/49

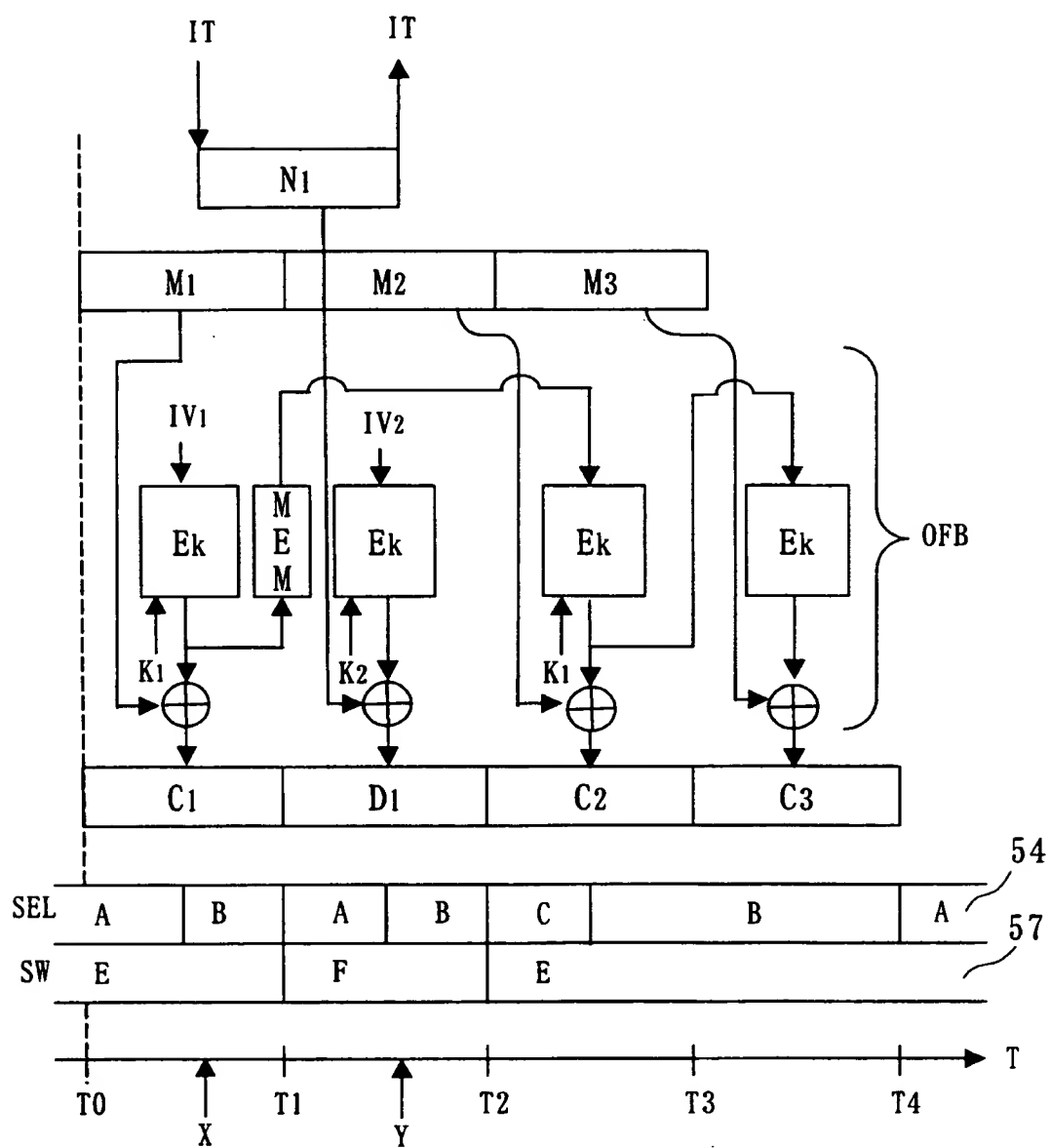
図 16



This Page Blank (uspto)

15/49

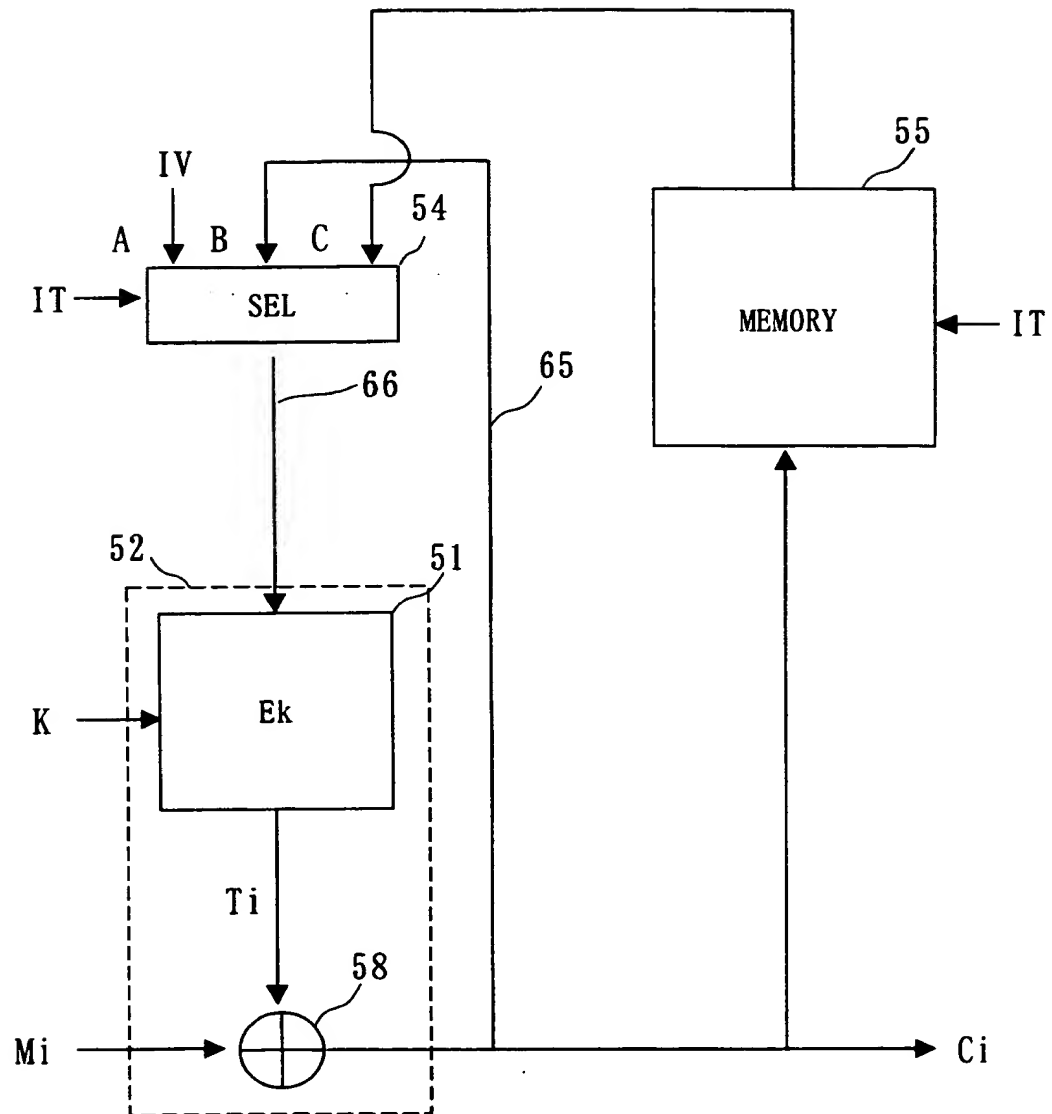
図 17



This Page Blank (uspto)

16/49

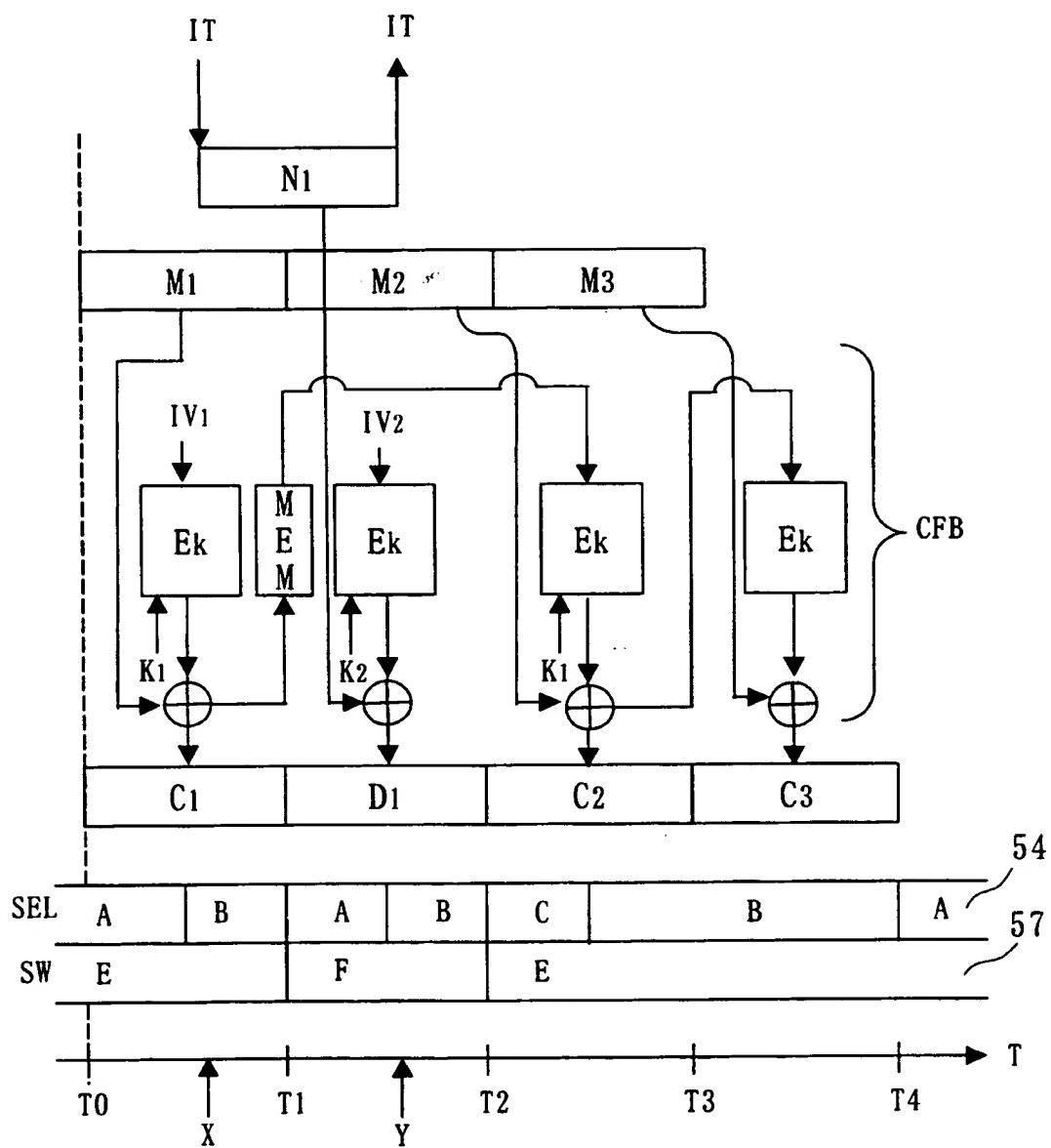
図 18



This Page Blank (uspto)

17/49

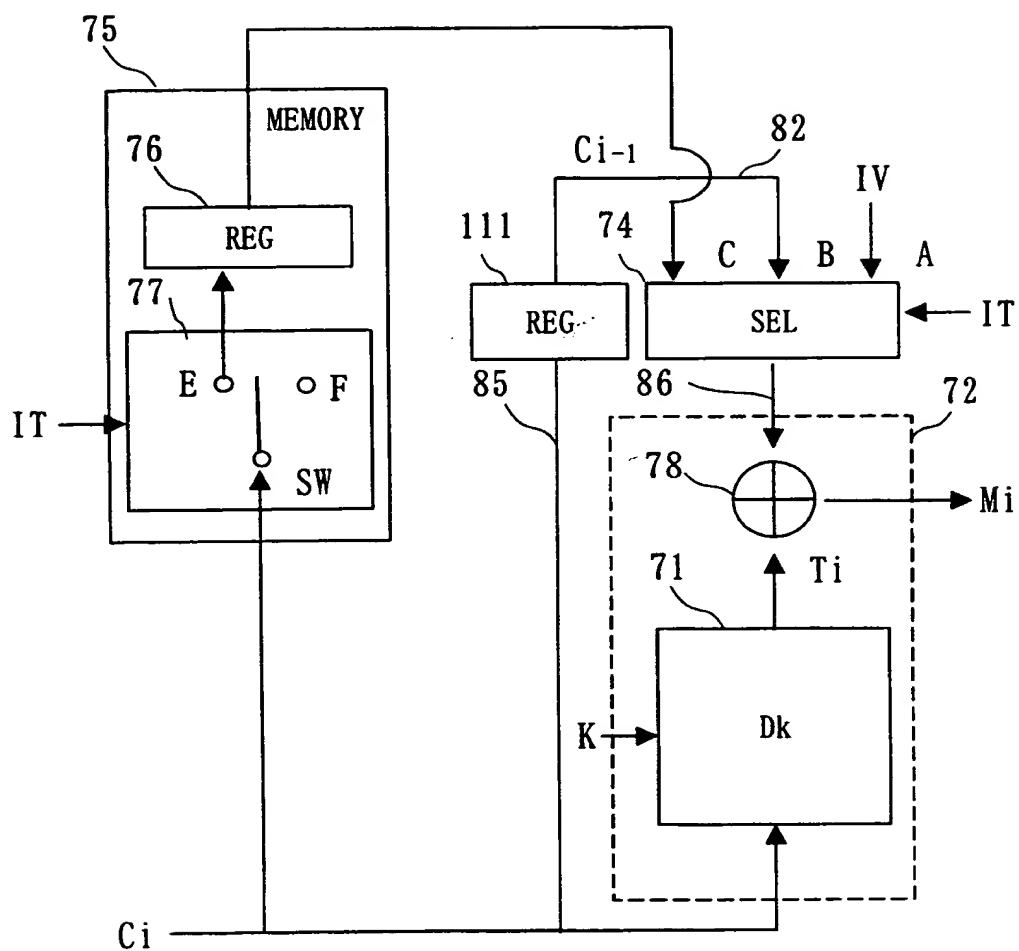
図 19



This Page Blank (uspto)

18/49

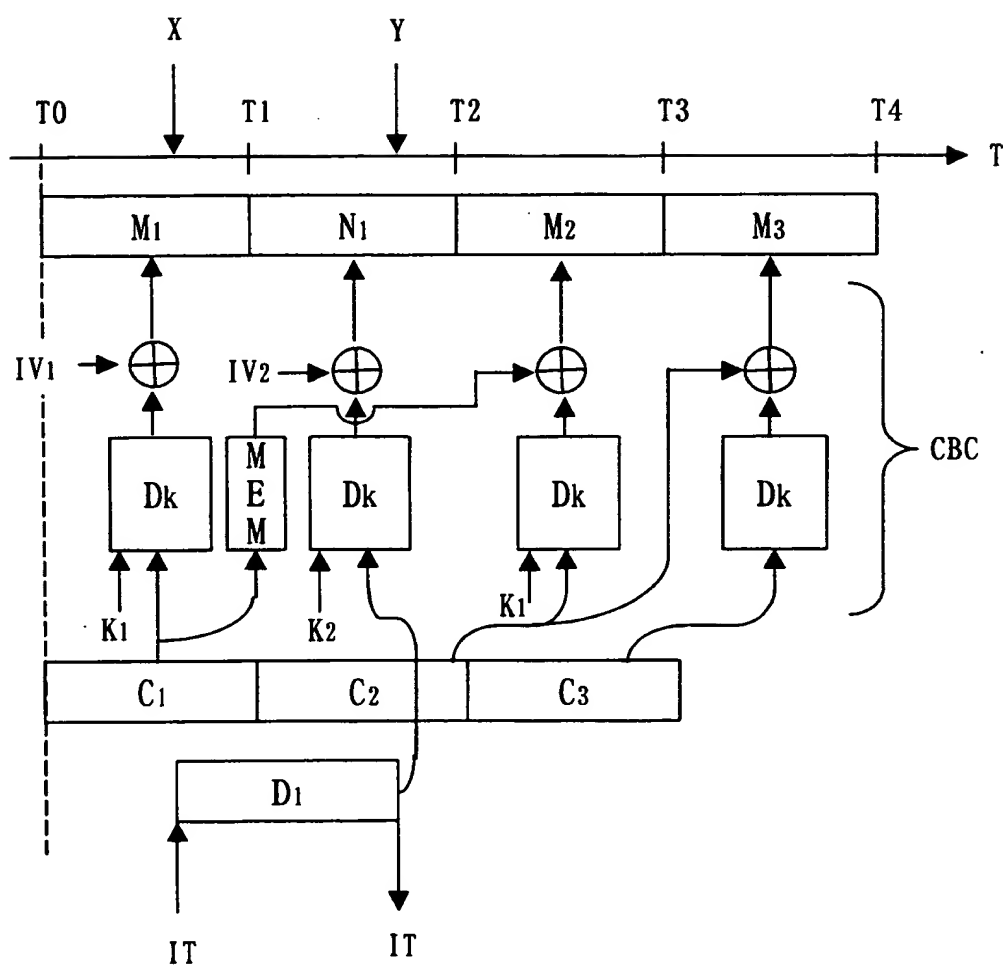
図 20



This Page Blank (uspto)

19/49

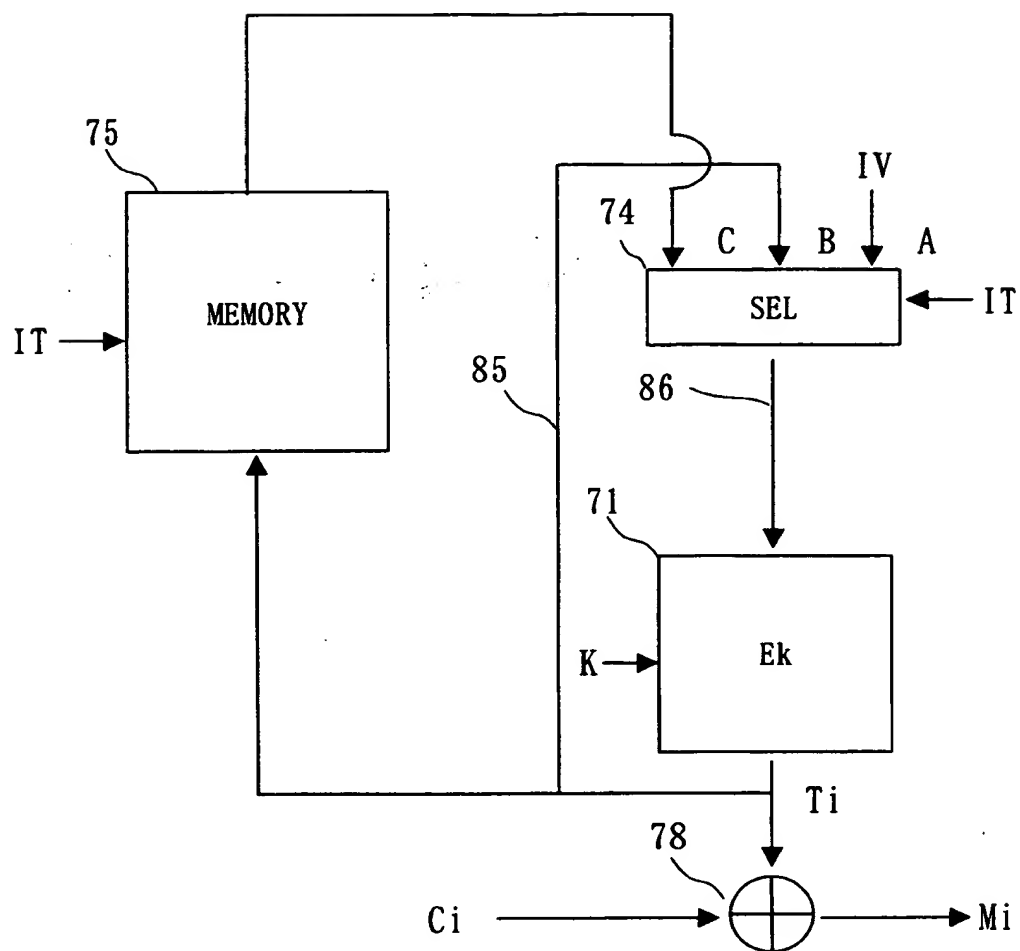
図21



This Page Blank (uspto)

20/49

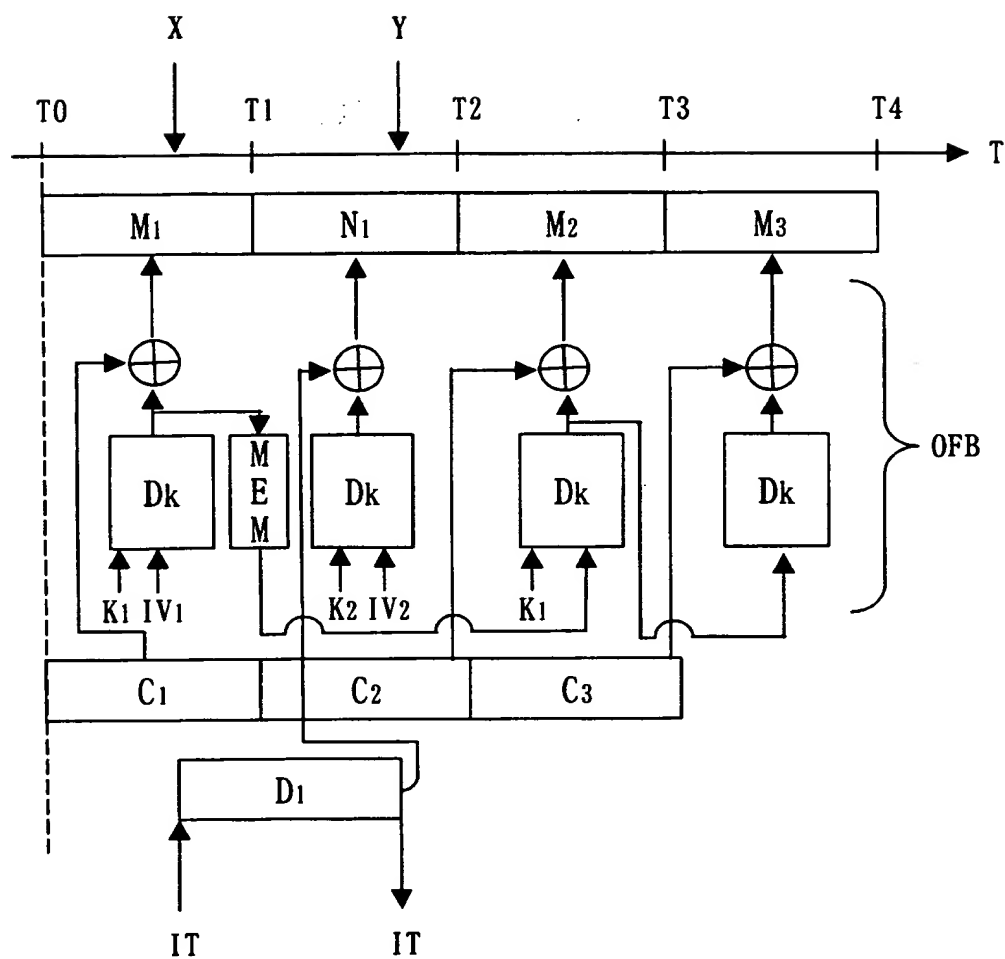
図22



This Page Blank (uspto)

21 / 49

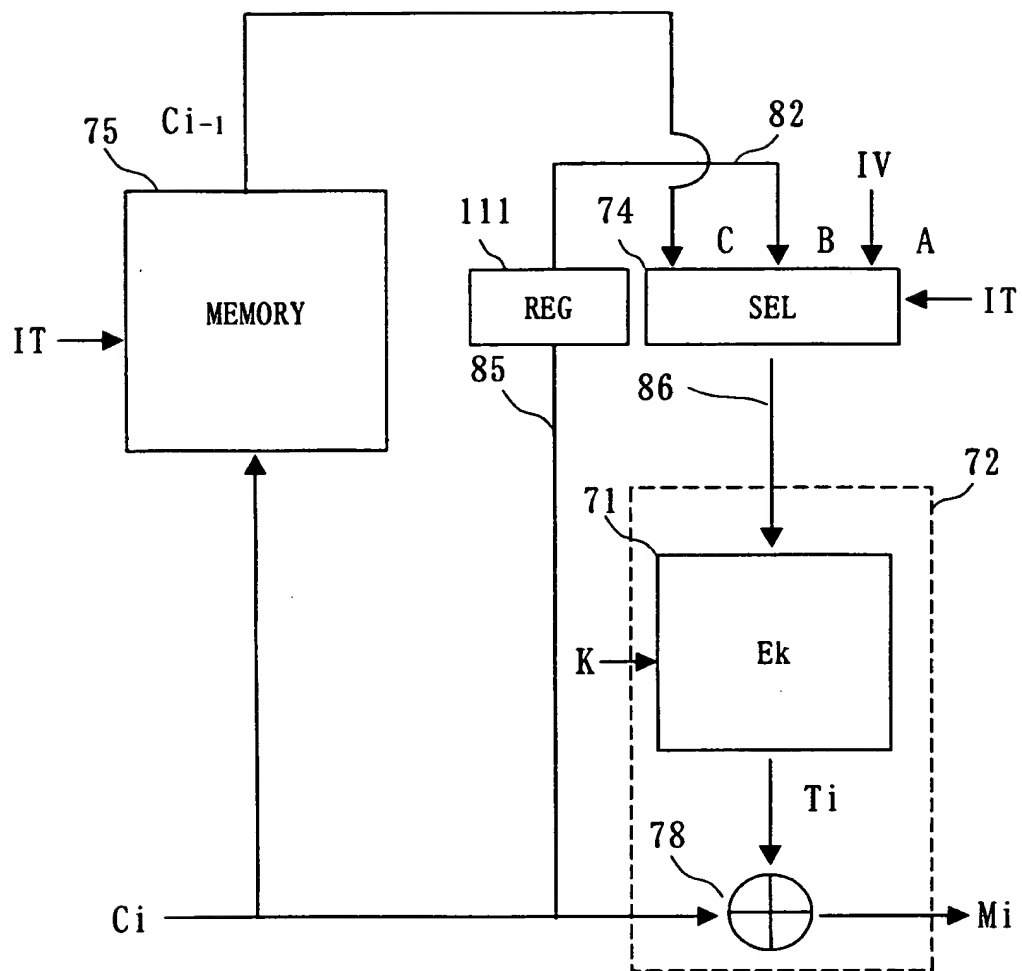
図 23



This Page Blank (uspto)

22/49

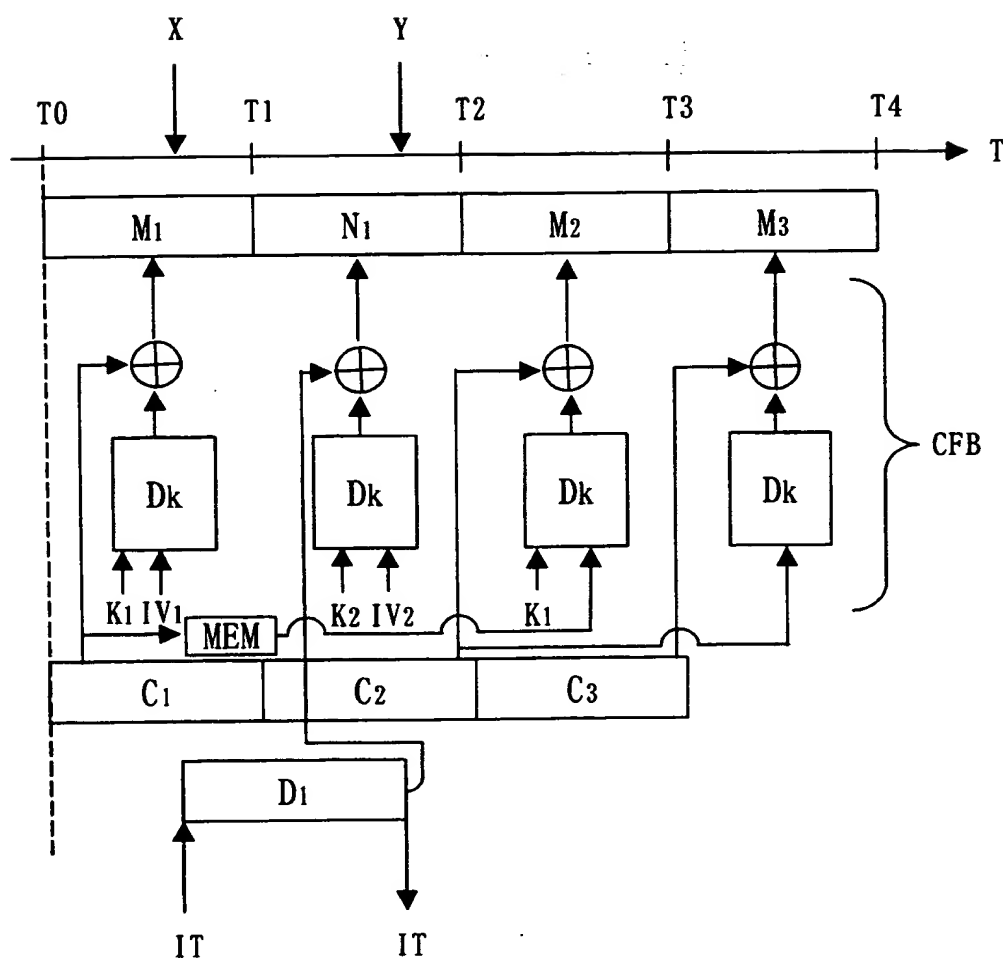
図 24



This Page Blank (uspto)

23/49

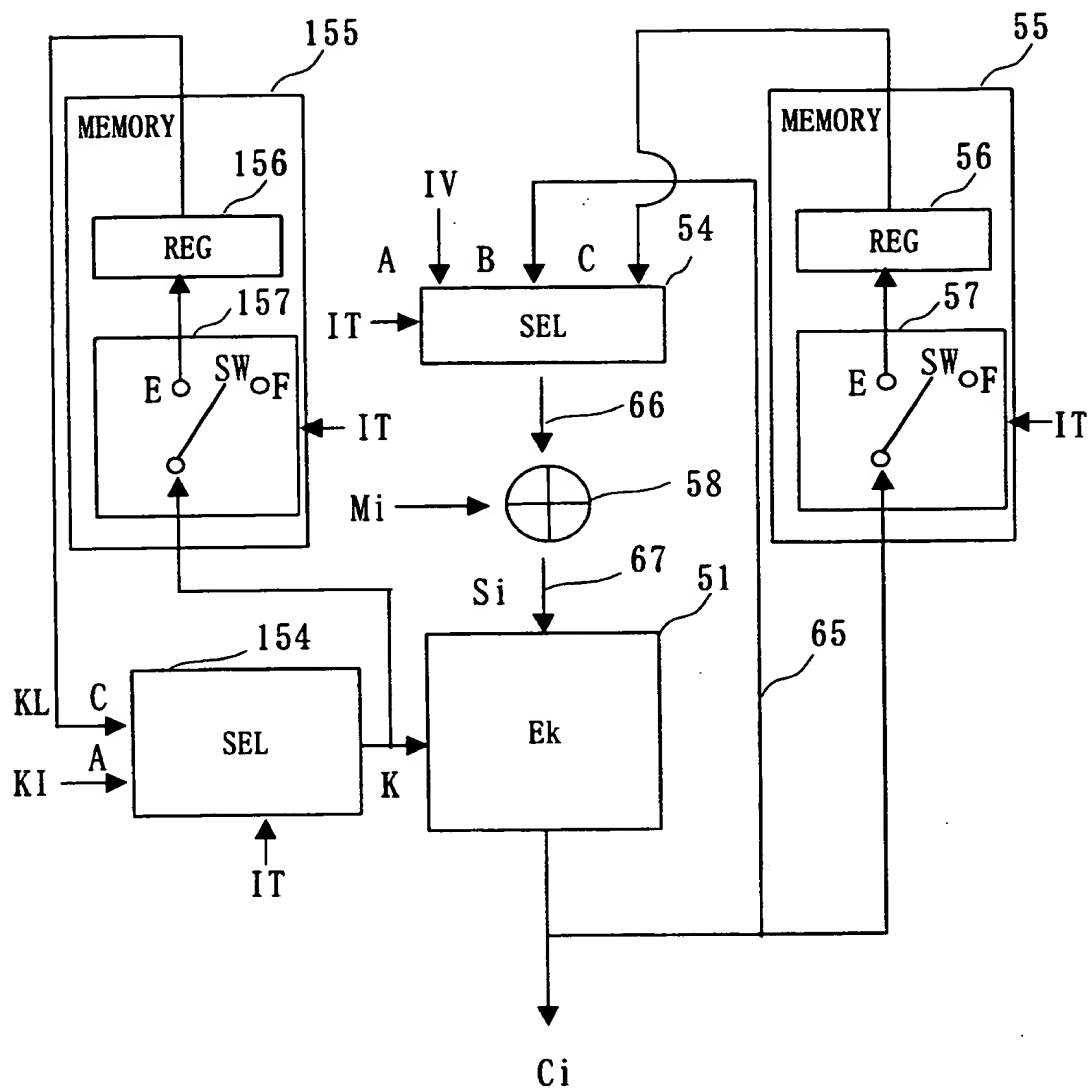
図 25



Inis Page Blank (uspto)

24/49

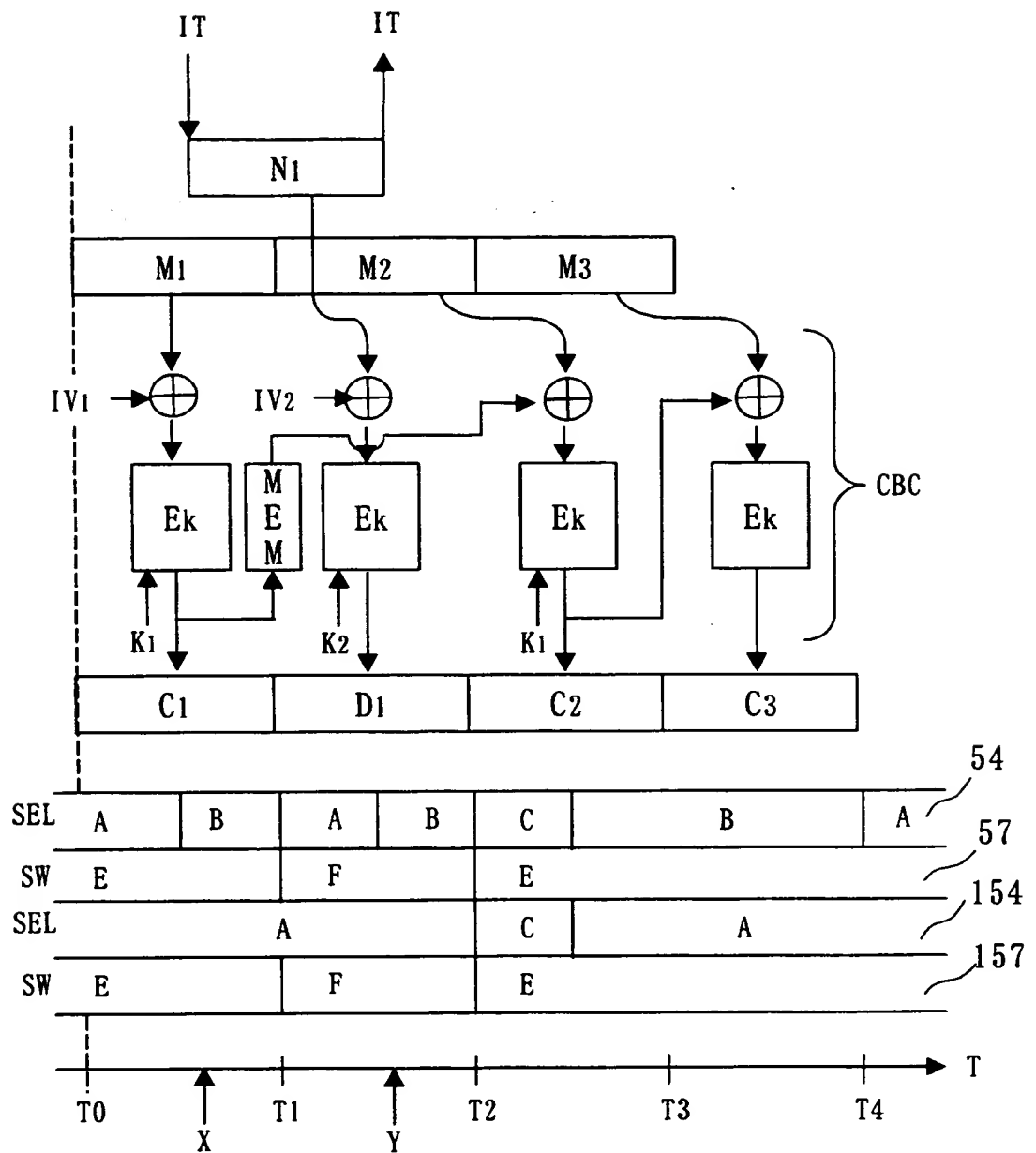
図26



This Page Blank (uspto)

25/49

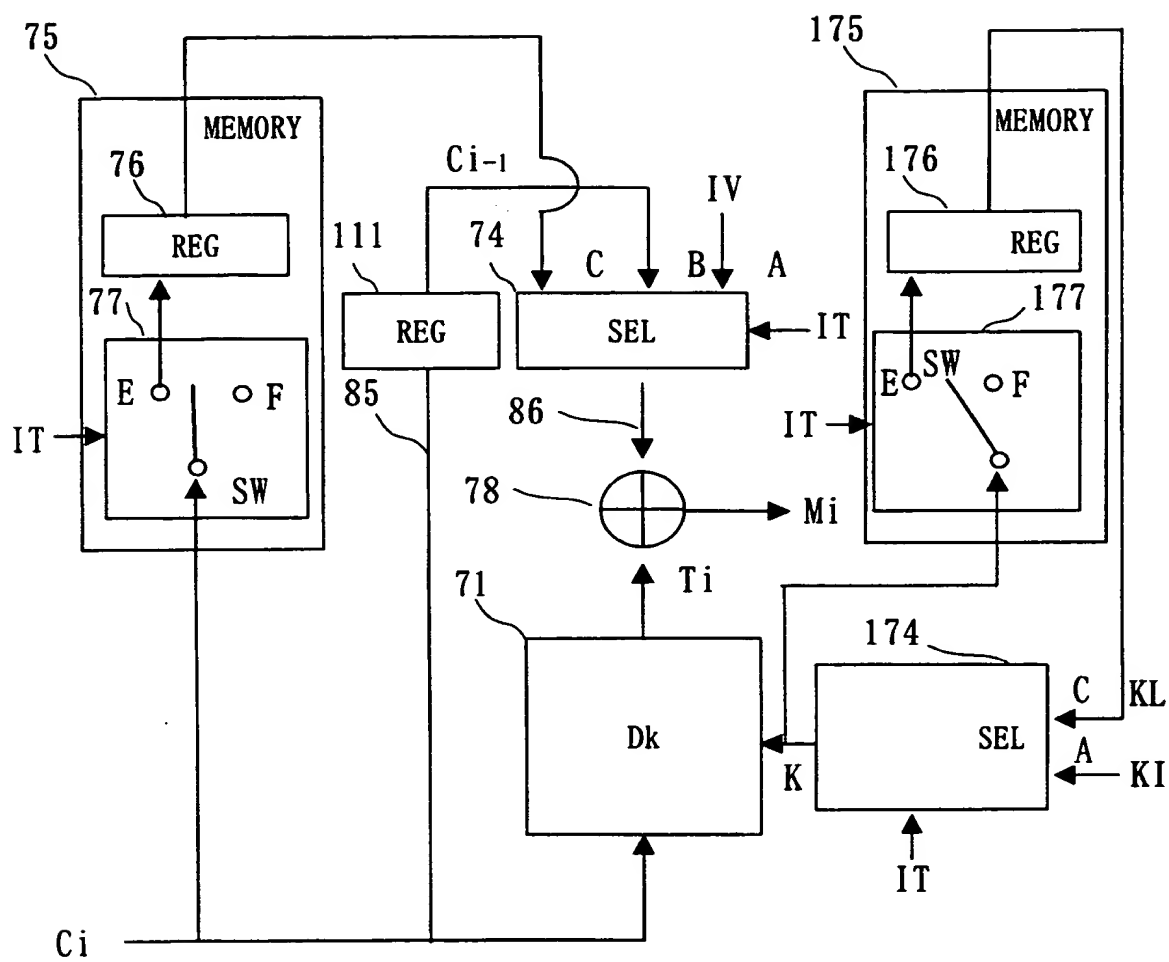
図 27



This Page Blank (uspto)

26/49

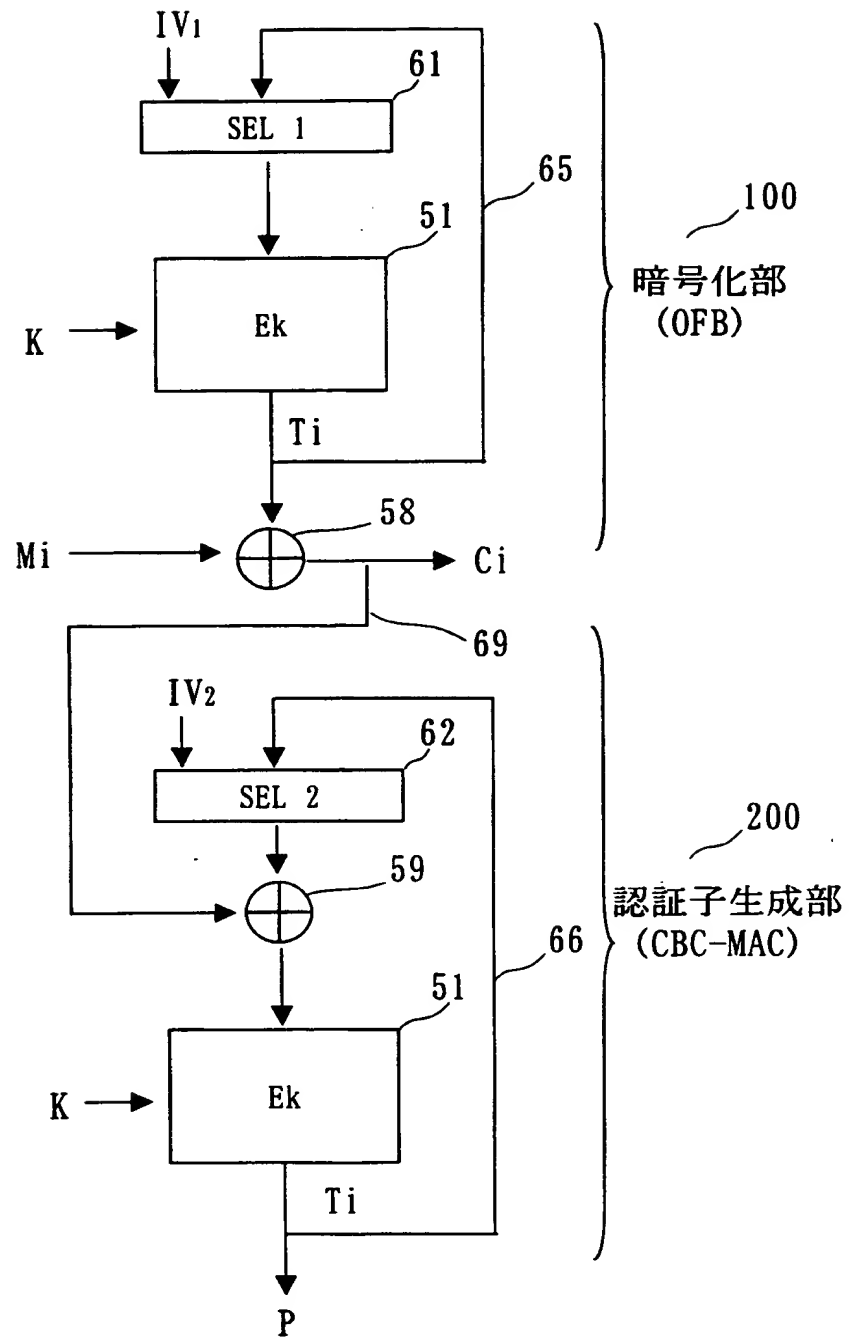
図 28



This Page Blank (uspto)

27/49

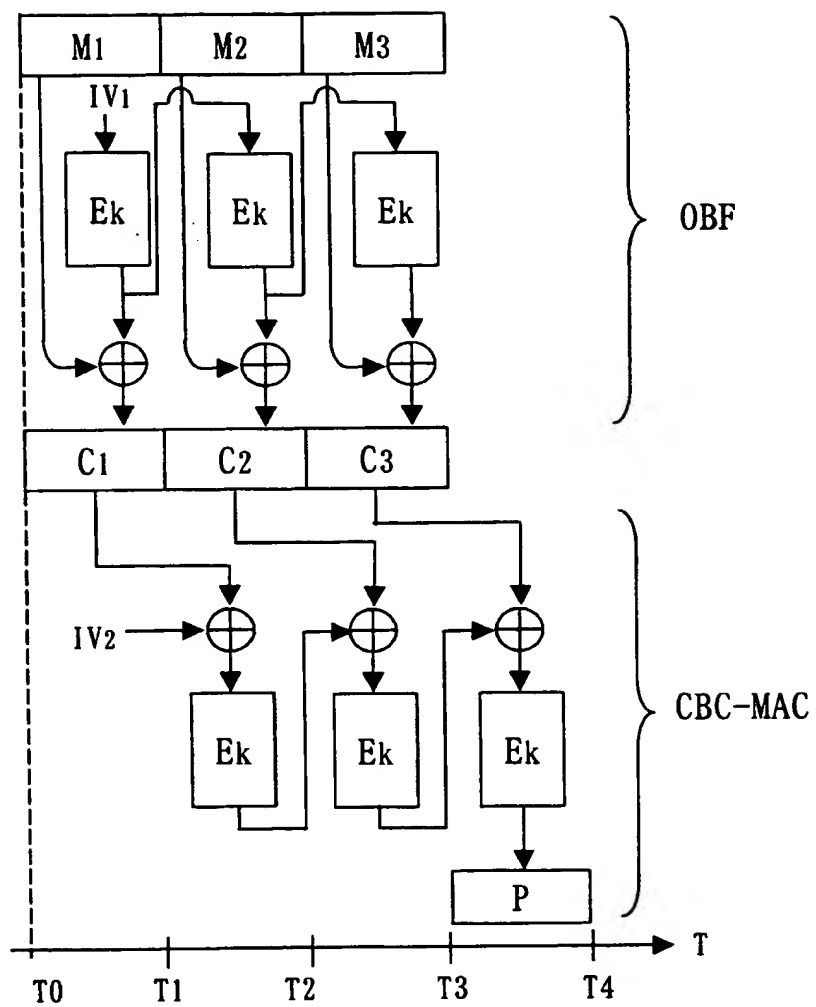
図 29



This Page Blank (uspto)

28/49

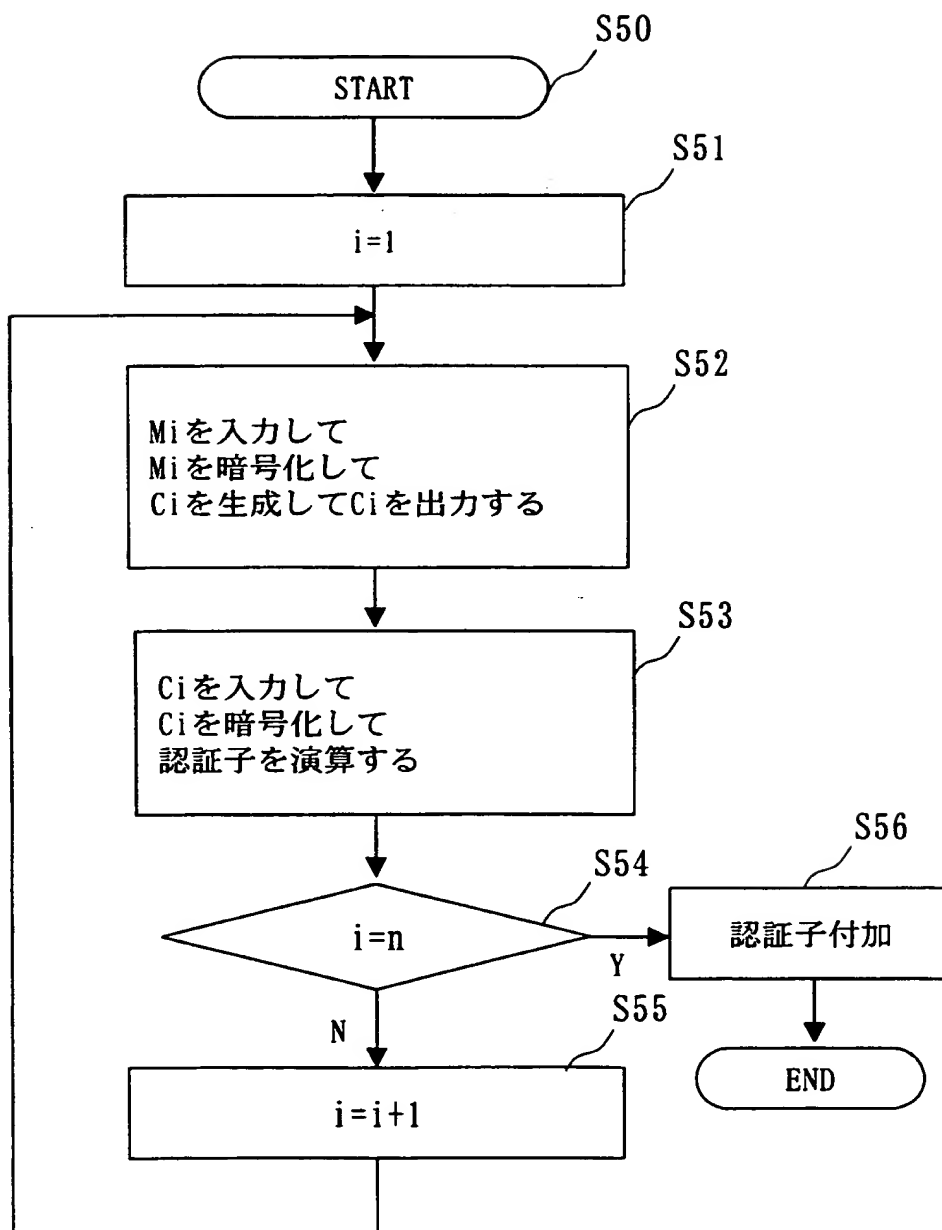
図 30



This Page Blank (uspto)

29 / 49

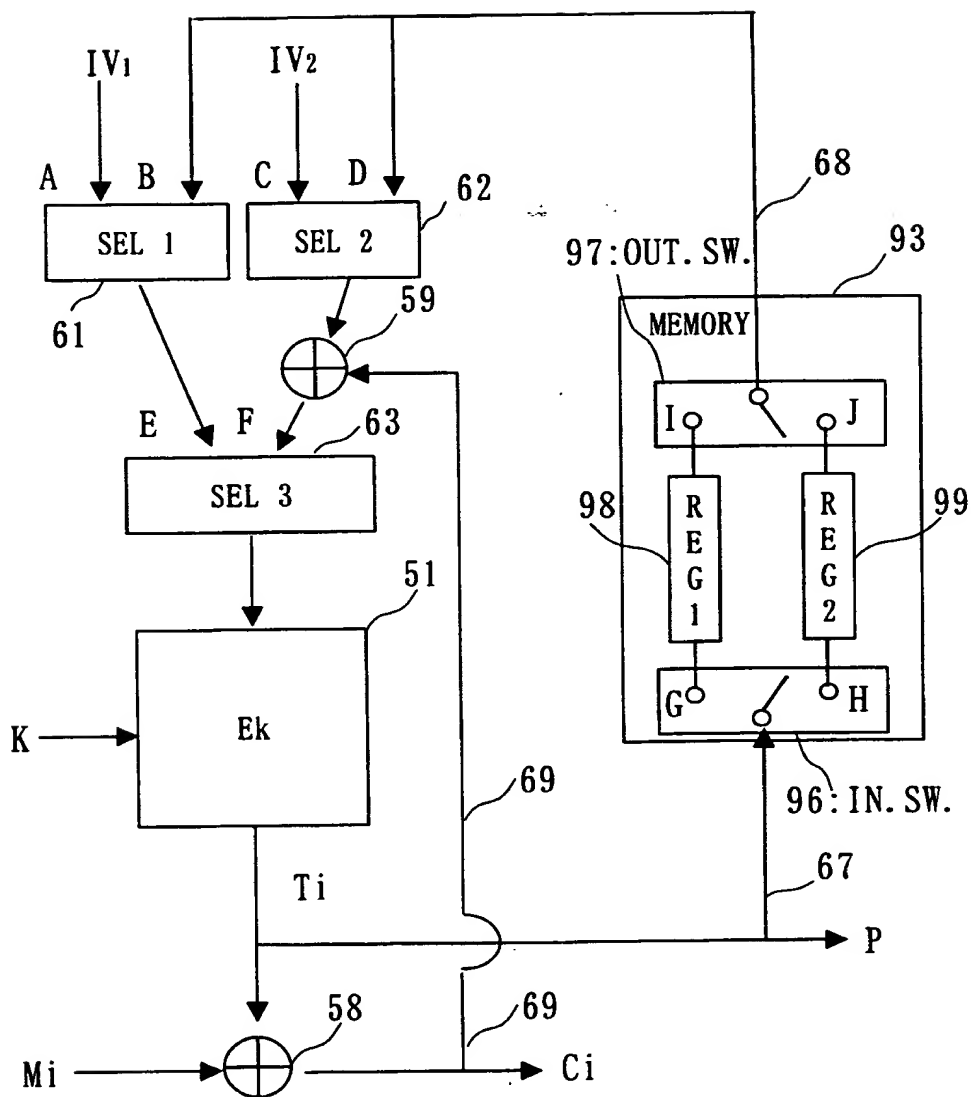
図31



This Page Blank (uspto)

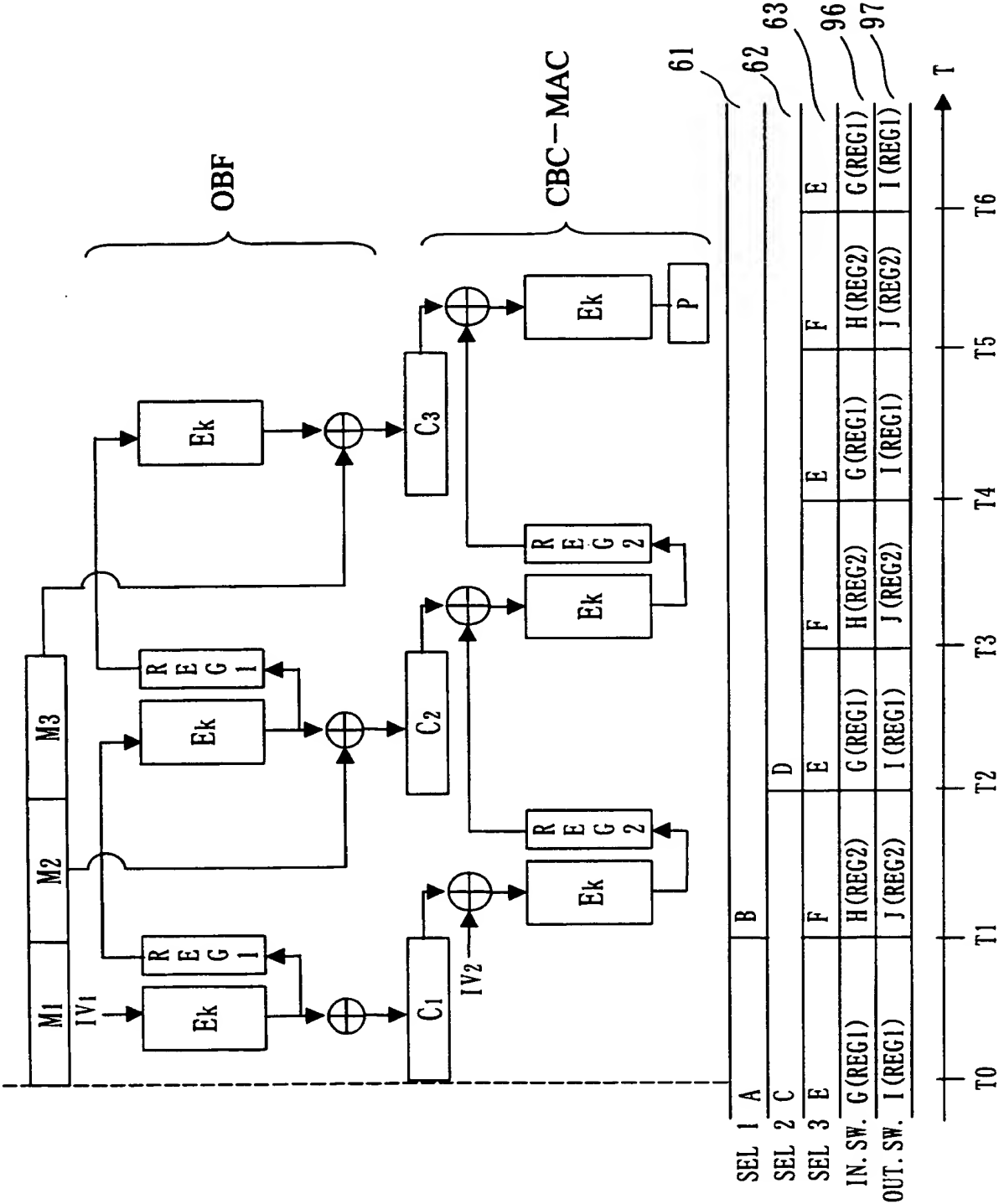
30/49

図 32



This Page Blank (uspto)

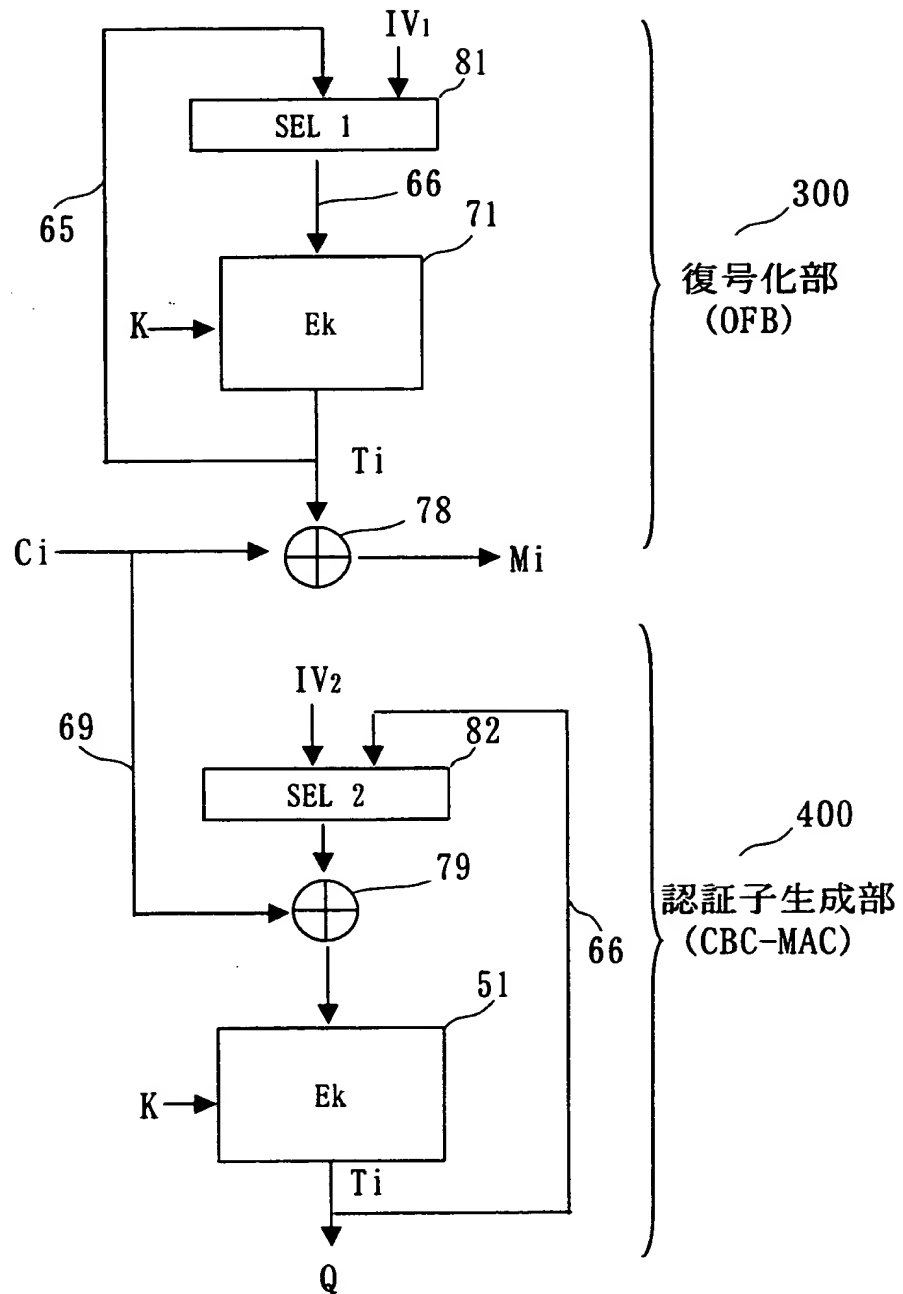
図 33



This Page Blank (uspto)

32 / 49

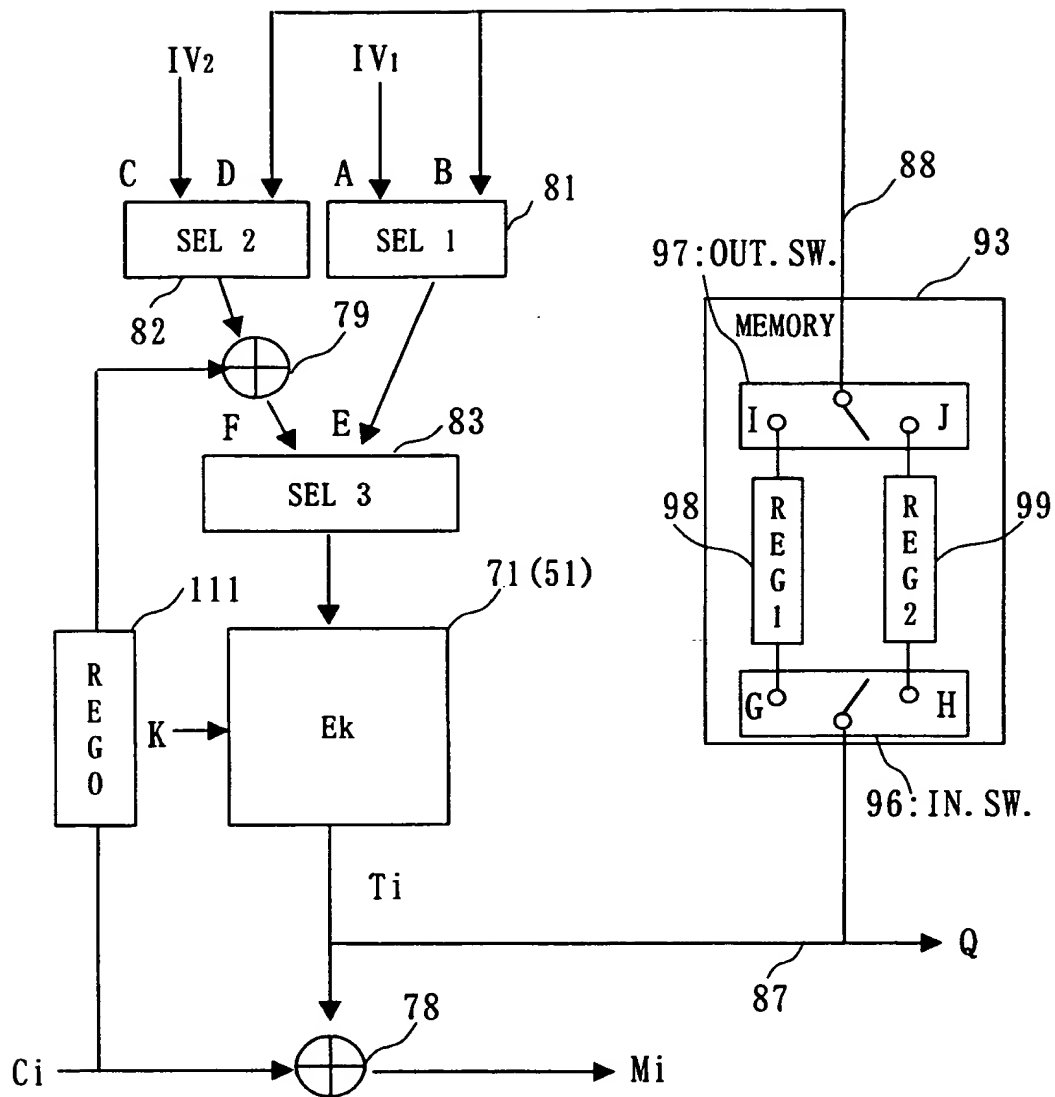
図 34



This Page Blank (uspto)

33/49

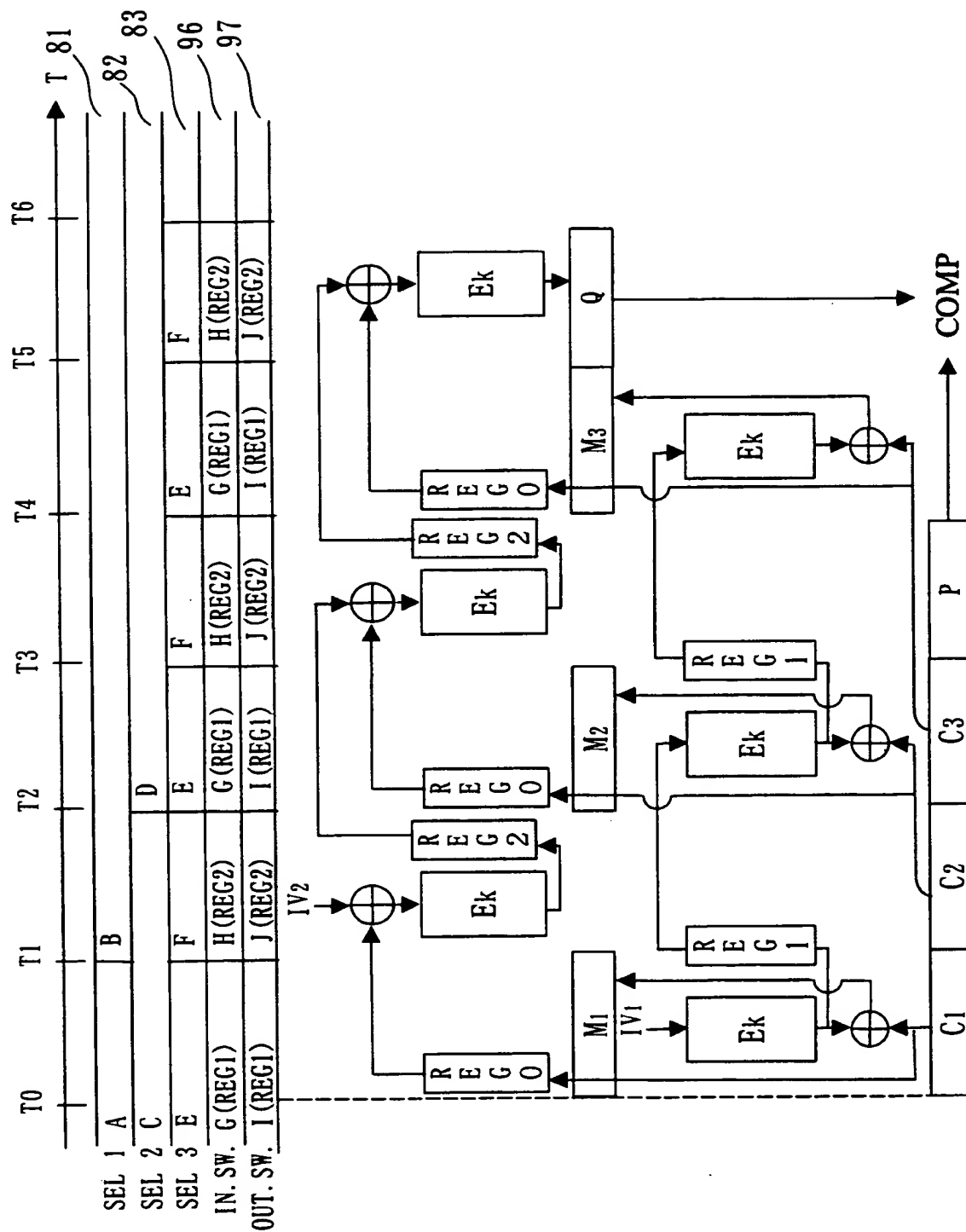
35



This Page Blank (uspto)

34 / 49

図 36

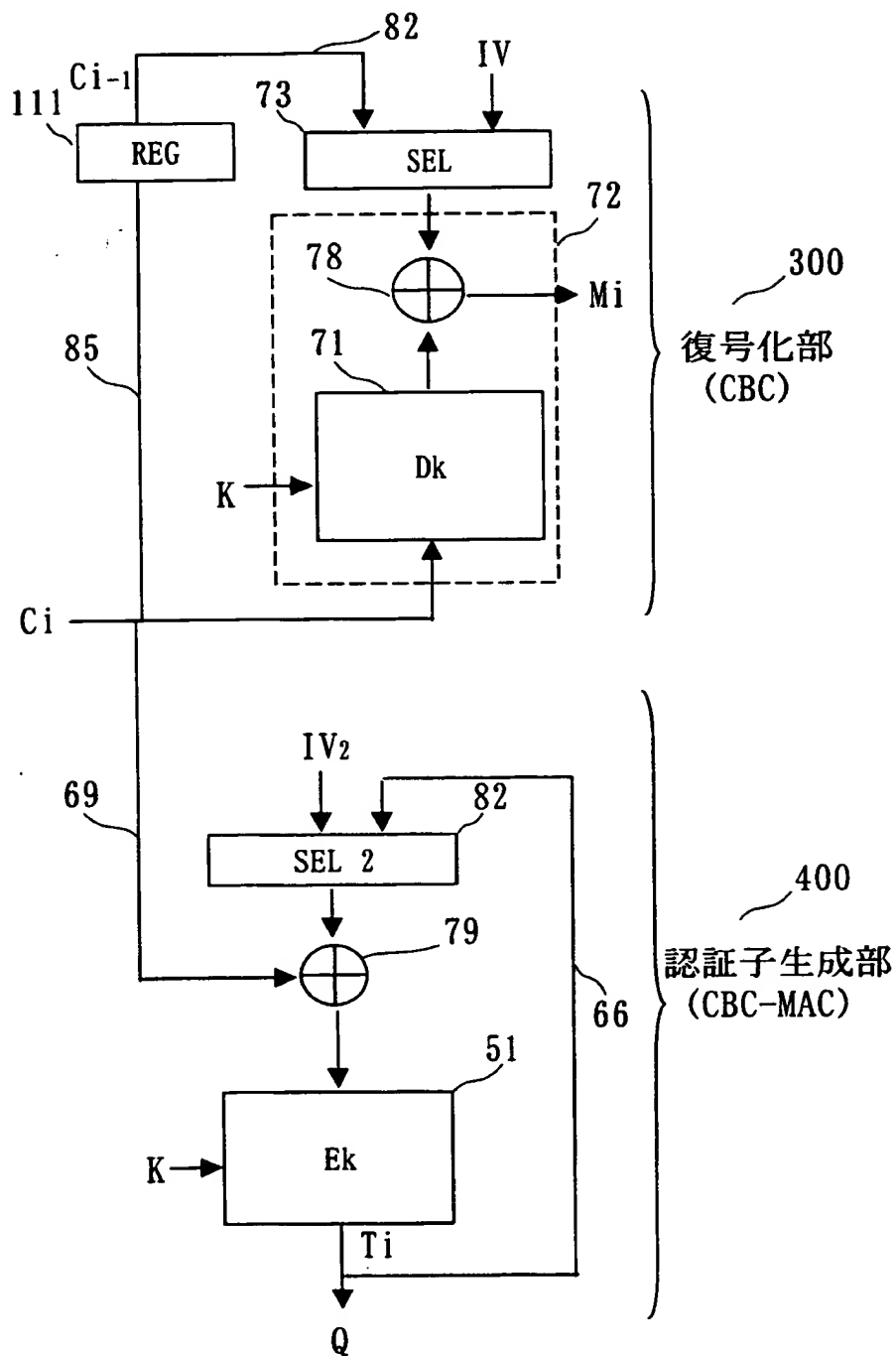


This Page Blank (uspto)

This Page Blank (uspto)

36/49

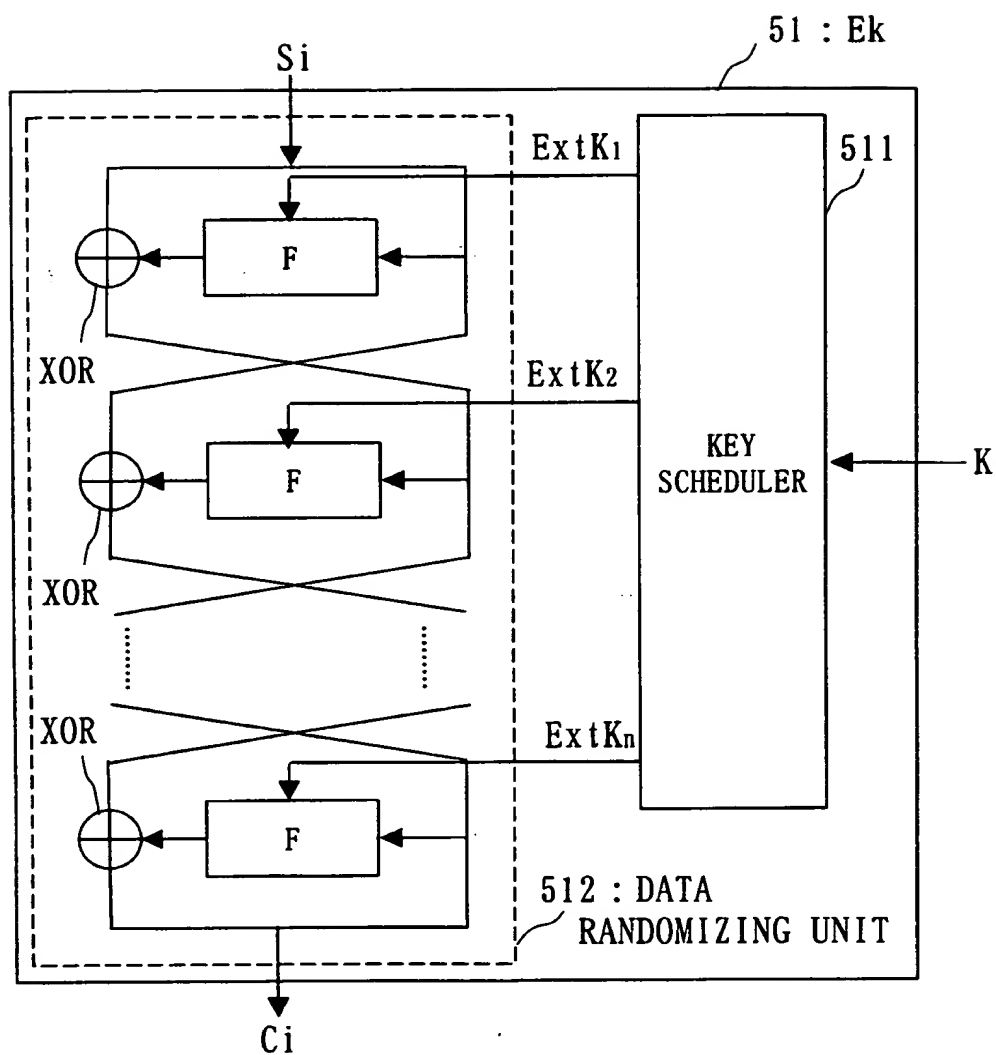
図 38



This Page Blank (uspto)

37/49

図 39



This Page Blank (uspto)

38/49

図40

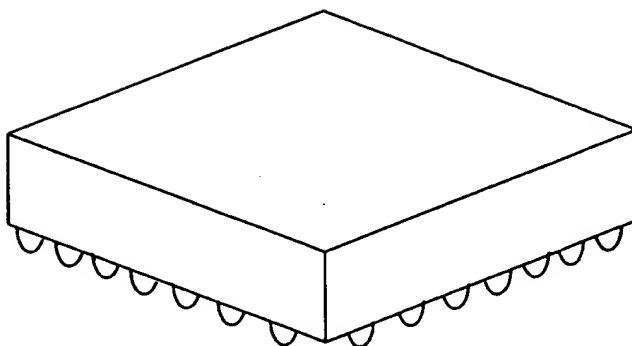
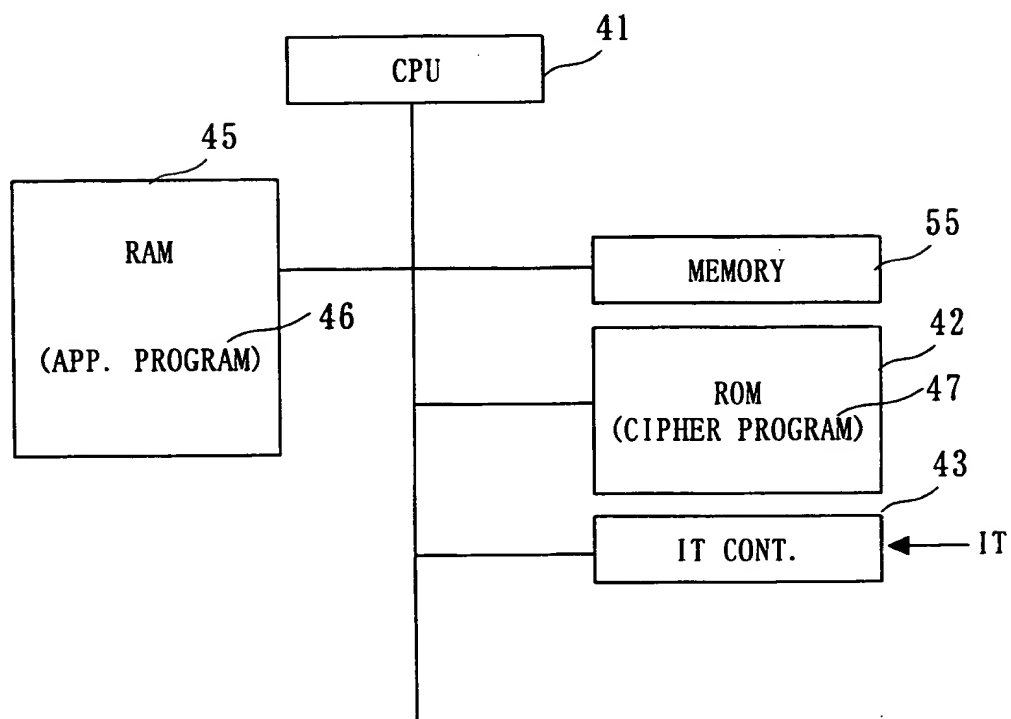


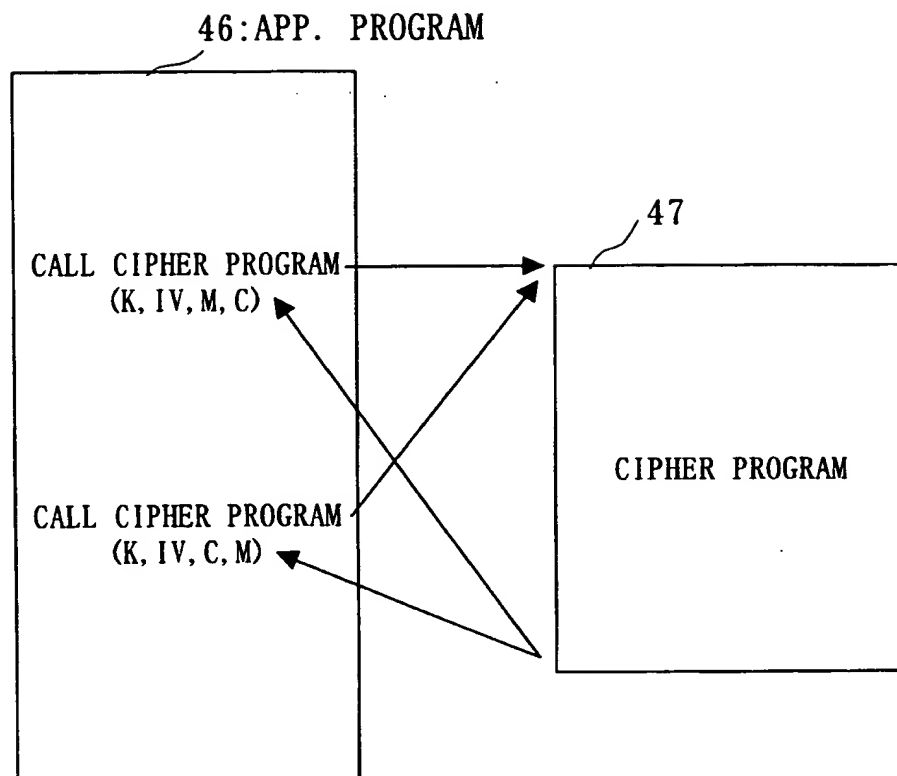
図41



This Page Blank (uspto)

39 / 49

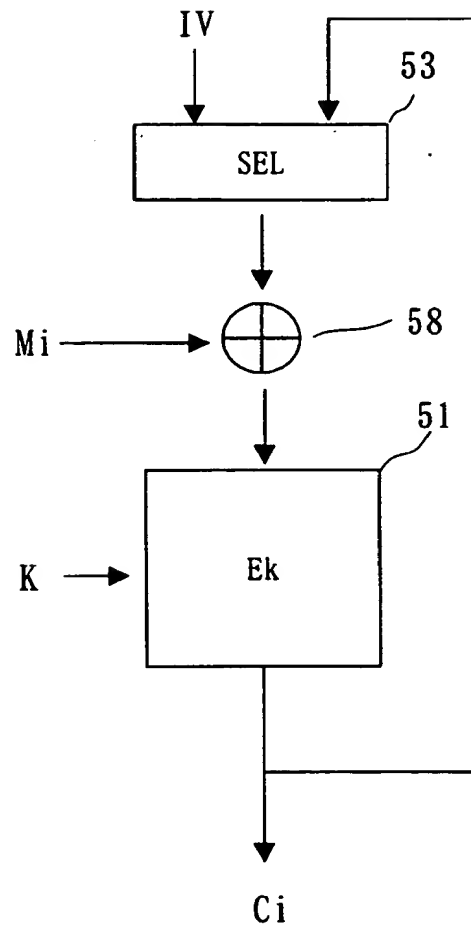
図 42



This Page Blank (uspto)

40/49

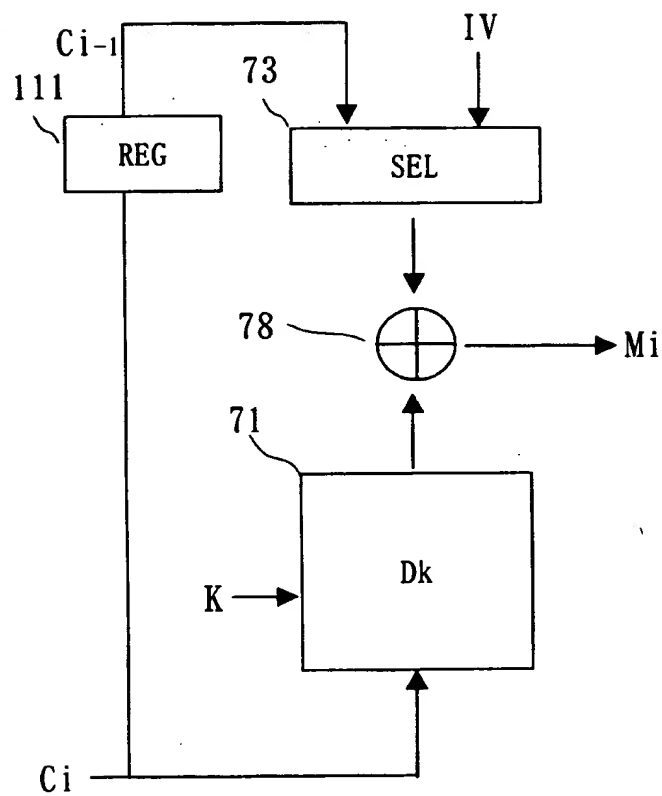
図43



This Page Blank (uspto)

41/49

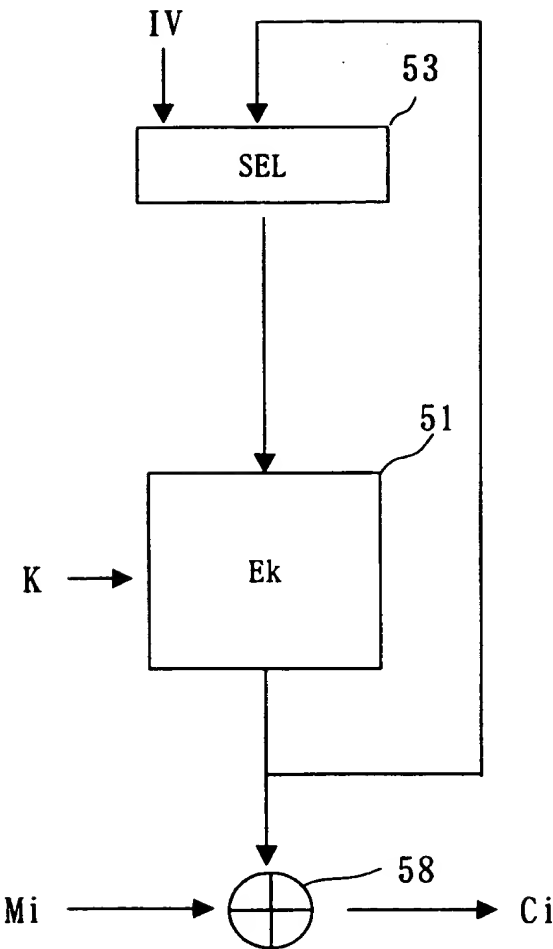
図44



This Page Blank (uspto)

42/49

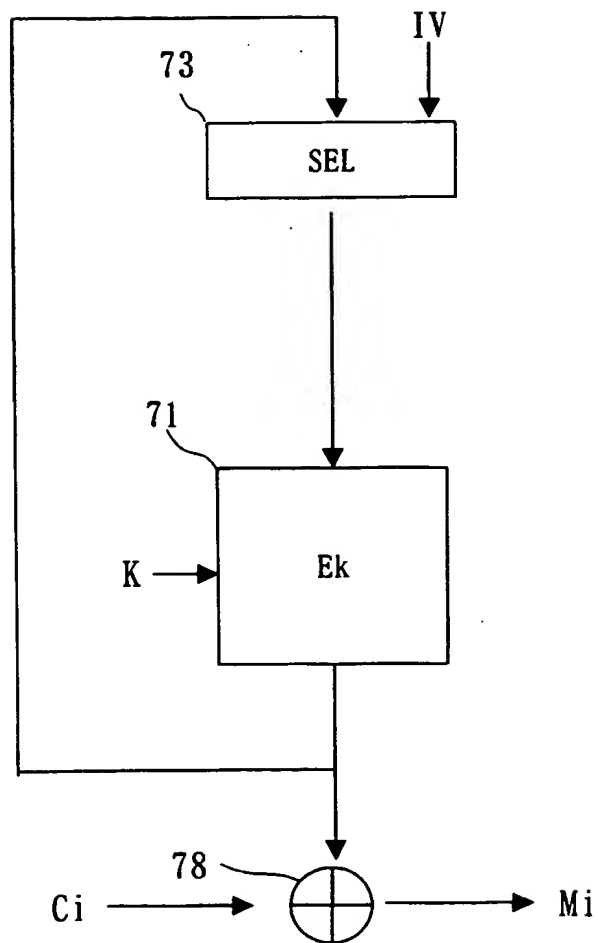
図45



This Page Blank (uspto)

43/49

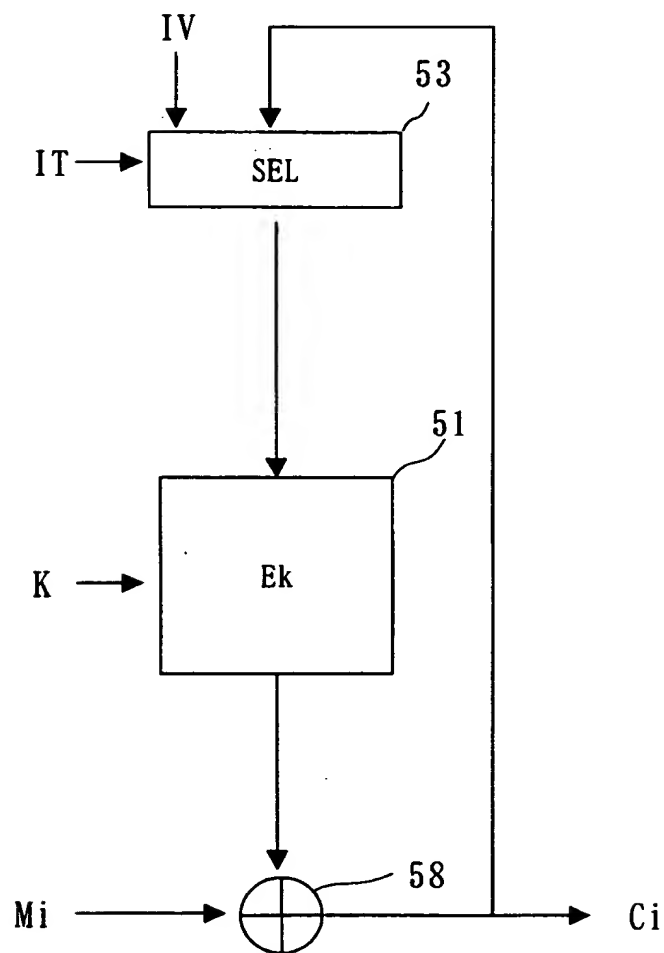
図46



This Page Blank (uspto)

44 / 49

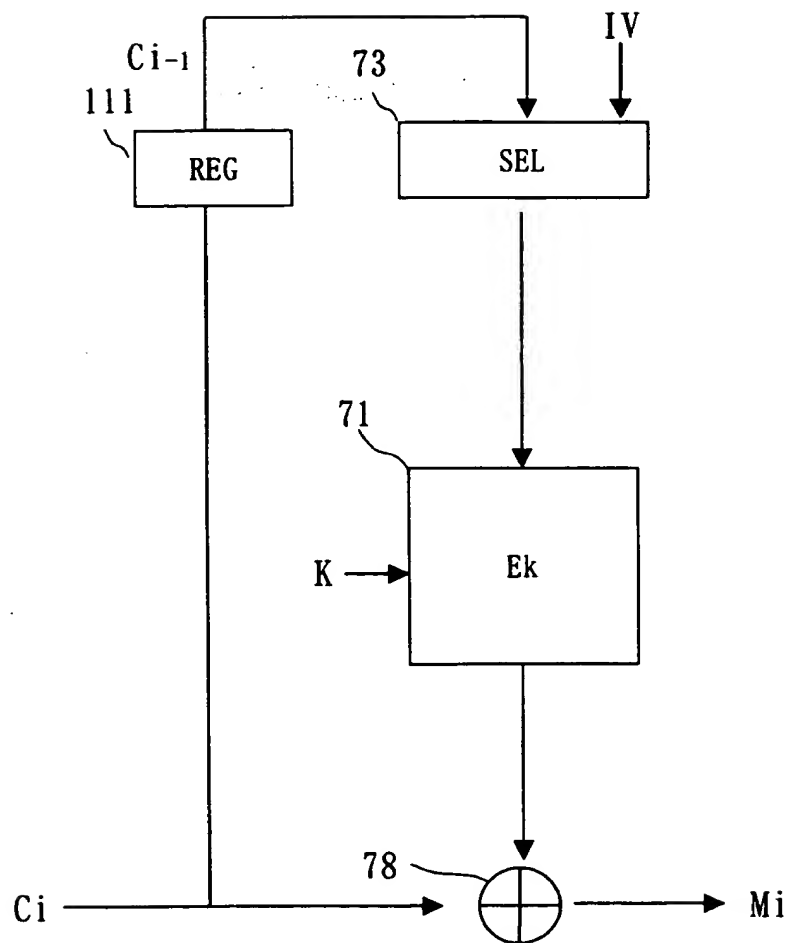
図 47



This Page Blank (uspto)

45/49

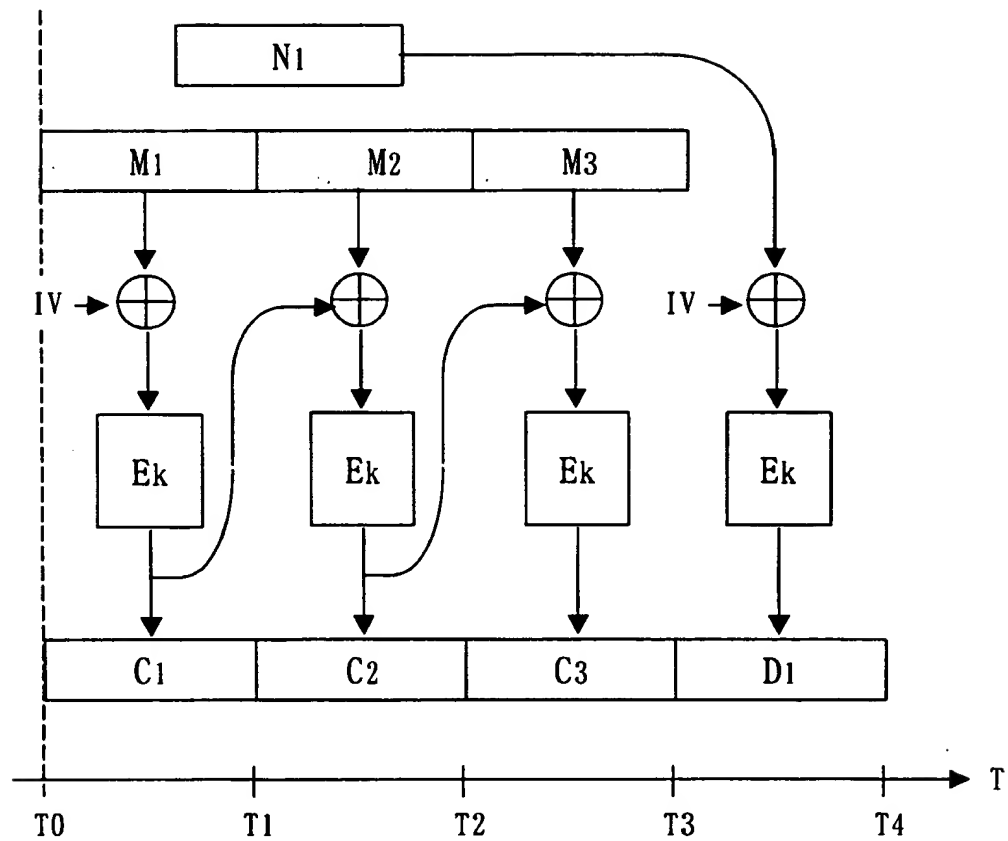
図 48



This Page Blank (uspto)

46 / 49

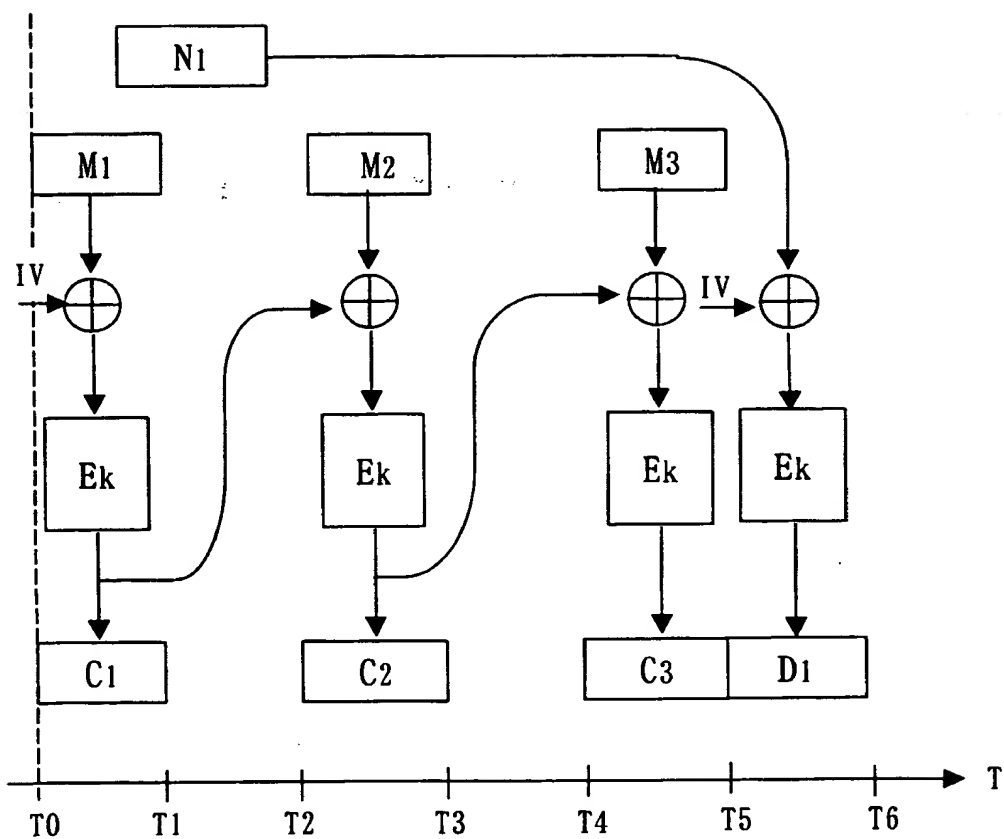
図 49



This Page Blank (uspto)

47/49

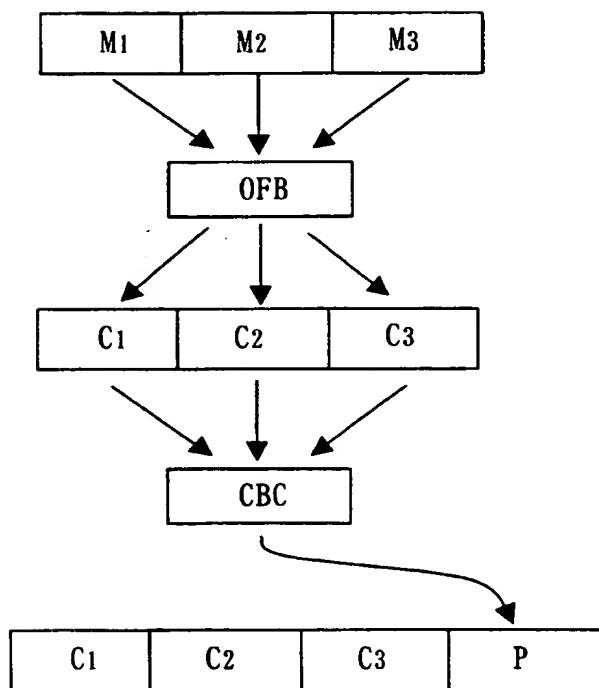
図 50



This Page Blank (uspto)

48/49

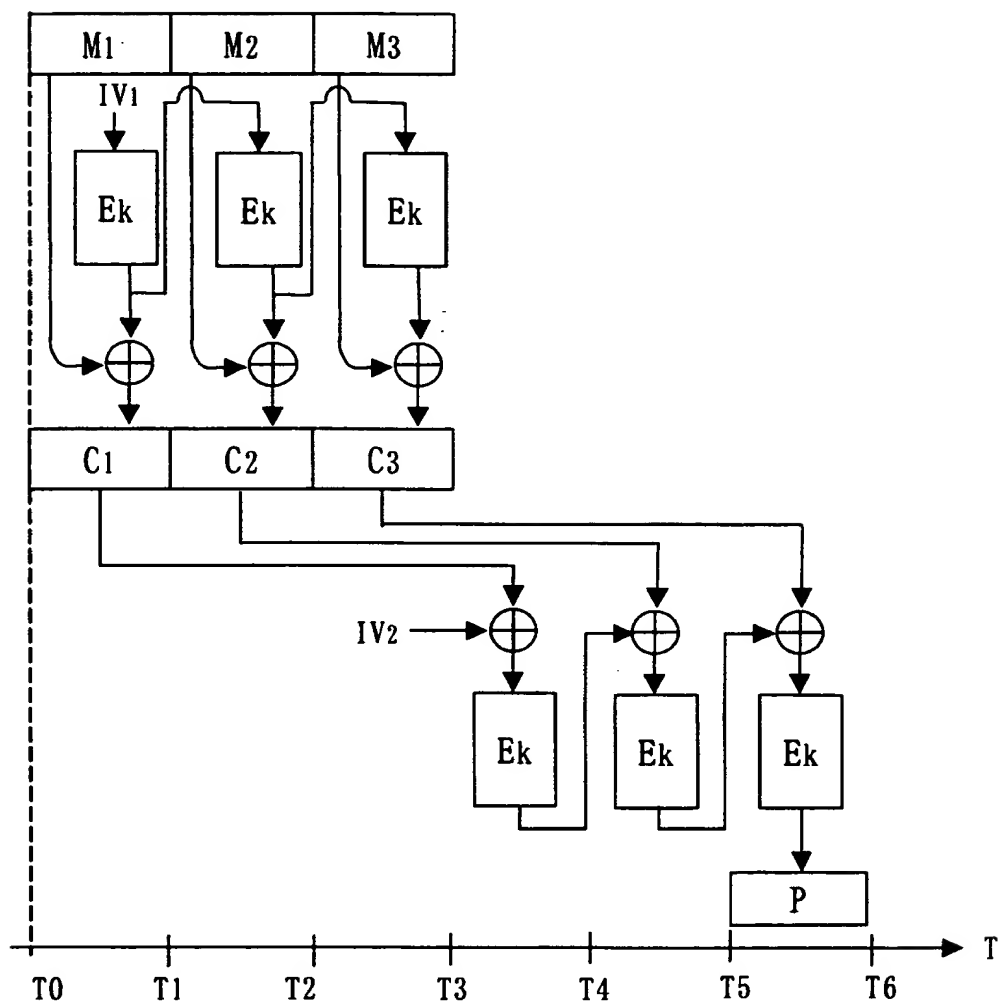
図51



This Page Blank (uspto)

49 / 49

図 52



This Page Blank (uspto)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/09129

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ H04L9/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2001

Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, 9-298736 (Matsushita Electric Ind. Co., Ltd.) 18 November, 1997 (18.11.97) page 10, right column, line 28 to page 12, left column, line 31; all drawings (Family: none)	1-7, 11-17, 21-23, 27-29, 33, 35, 37, 39, 41-44
X	JP, 10-123950, A (Fuji Xerox Co., Ltd.), 15 May, 1998 (15.05.98), page 4, right column, line 38 to page 5, left column, line 27; Fig. 21	8, 10, 18, 20, 24, 26, 30, 32, 34, 36, 38, 40, 45-50
A	Full text; all drawings & EP, 837383, A2 & US, 6161183, A	9, 19, 25, 31
X	JP, 8-248879, A (International Business Machines Corp.), 27 September, 1996 (27.09.96), page 4, right column, lines 33 to 43; all drawings & EP, 725511, A2 & US, 5673319, A1	8-10, 18-20, 24-26, 30-32, 34, 36, 38, 40, 45-50



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T"

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X"

document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y"

document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"

document member of the same patent family

Date of the actual completion of the international search
30 March, 2001 (30.03.01)Date of mailing of the international search report
10 April, 2001 (10.04.01)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/09129

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 4-48336, A (Fujitsu Limited), 18 February, 1992 (18.02.92), Full text; all drawings (Family: none)	1-50
A	JP, 2-73747, A (NEC Corporation), 13 March, 1990 (13.03.90), Full text; Fig. 1 (Family: none)	1-50
A	JP, 57-69344, A (Nippon Telegr. & Teleph. Corp. <NTT>), 28 April, 1982 (28.04.82), Full text; all drawings (Family: none)	1-50
A	JP, 4-191935, A (Toshiba Corporation), 10 July, 1992 (10.07.92), Full text; all drawings (Family: none)	1-50

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/10

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年
 日本国公開実用新案公報 1971-2001年
 日本国登録実用新案公報 1994-2001年
 日本国実用新案登録公報 1996-2001年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	J P, 9-298736 (松下電器産業株式会社) 18. 11月. 1997 (18. 11. 97) 第10頁右欄第28行目~第12頁左欄第31行目, 全図 (ファミリーなし)	1-7, 11-17, 21-23, 27-29, 33, 35, 37, 39, 41-44

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」 口頭による開示、使用、展示等に言及する文献
 「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」 同一パテントファミリー文献

国際調査を完了した日

30. 03. 01

国際調査報告の発送日

10.04.01

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)
 郵便番号100-8915
 東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5W

2956

電話番号 03-3581-1101 内線 3535

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	J P, 10-123950, A (富士ゼロックス株式会社) 15. 5月. 1998 (15. 05. 98) 第4頁右欄第38行目~第5頁左欄第27行目, 第21図	8, 10, 18, 20, 24, 26, 30, 32, 34, 36, 38, 40, 45-50
A	全文, 全図 & EP, 837383, A2 & US, 6161183, A	9, 19, 25, 31
X	J P, 8-248879, A (インターナショナル・ビジネス・マ シーンズ・コーポレーション) 27. 9月. 1996 (27. 09. 96) 第4頁右欄第33行目~第43行目, 全図 & EP, 725511, A2 & US, 5673319, A1	8-10, 18-20, 24-26, 30-32, 34, 36, 38, 40, 45-50
A	J P, 4-48336, A (富士通株式会社) 18. 2月. 1992 (18. 02. 92) 全文, 全図 (ファミリーなし)	1-50
A	J P, 2-73747, A (日本電気株式会社) 13. 3月. 1990 (13. 03. 90) 全文, 第1図 (ファミリーなし)	1-50
A	J P, 57-69344, A (日本電信電話公社) 28. 4月. 1982 (28. 04. 82) 全文, 全図 (ファミリーなし)	1-50
A	J P, 4-191935, A (株式会社東芝) 10. 7月. 1992 (10. 07. 92) 全文, 全図 (ファミリーなし)	1-50